Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Critical Infrastructure References Documented Literature Search

Kyungryun (Cathy) Pak
Lynne Genik
DRDC Centre for Security Science

Disclaimer: The inclusion of a particular tool or methodology in this literature search should not be considered as an endorsement by DRDC. It is highly recommended that the references be reviewed before being applied or used in particular contexts or situations.

Defence R&D Canada – Centre for Security Science
Technical Note
DRDC CSS TN 2012-013
October 2012

Canada

Principal Author

Kyungryun (Cathy) Pak

DRDC Centre for Security Science

Approved by

Dr. Denis Bergeron

DRDC Centre for Security Science
Head Decision Support Section

Approved for release by

Dr. Mark Williamson

DRDC Centre for Security Science
Document Review Panel Chairman

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2012

© Sa Majesté la Reine (en droit du Canada), telle que représentée par le ministre de la Défense nationale, 2012

Abstract

This document presents the results of a literature search on critical infrastructure (CI), an initiative undertaken by Defence Research and Development Canada (DRDC) as a part of its collaborative project with Emergency Management British Columbia (EMBC). The literature search document comprises a collection of approximately 200 references, including bibliographic information, abstracts, and content descriptions. In addition, the references are organized into the following categories: national approaches to CI; processes for managing CI; incident case studies and lessons learned; business continuity; and miscellaneous references. The references include government publications, academic papers, and the work of non-governmental and private sector organizations. These references were categorized, ordered, and described to allow readers to identify and retrieve references that are most valuable to their work and interests, and is thus intended to serve as a resource for DRDC, EMBC and other partners.

Résumé

Le présent document expose les résultats d'une recherche documentaire sur les infrastructures essentielles (IE), une initiative de Recherche et développement pour la défense Canada (RDDC) dans le cadre de son projet de collaboration avec Emergency Management British Columbia (EMBC). La recherche documentaire comporte une collection d'environ 200 références, y compris des renseignements bibliographiques, des résumés et des descriptions de contenu. En outre, les références sont classées dans les catégories suivantes : approches nationales aux IE; processus de gestion des IE; études de cas d'incident et leçons apprises; continuité des activités; références diverses. Les références comprennent des publications gouvernementales, des documents universitaires et des travaux d'organismes non gouvernementaux et du secteur privé. Ces références ont été classées par catégories et ordonnées et ont fait l'objet de descriptions afin de permettre aux lecteurs de repérer et de récupérer les références les plus utiles pour ce qui est de leur travail et de leurs intérêts. Par conséquent, elles ont pour but de servir de ressources pour RDDC, EMBC et d'autres partenaires.

Executive summary

Critical Infrastructure References: Documented Literature Search

Kyungryun (Cathy) Pak, Lynne Genik, DRDC Centre for Security Science; DRDC CSS TN 2012-013; Defence R&D Canada – CSS; October 2012.

Background: The aim of the collaborative project between Emergency Management British Columbia (EMBC) and Defence Research and Development Canada (DRDC) is to improve emergency management capabilities by applying and demonstrating the value of a scientific approach. The project focuses primarily on risk assessment (RA) and critical infrastructure (CI), and literature reviews in these two areas were conducted in the initial phase of the project. However, DRDC identified the potential value of more extensive reviews, and as a result, thorough literature searches were conducted and documented. This paper presents the results of the literature search for CI.

Method: The literature search was primarily conducted using online databases such as the DRDC research database and the University of Ottawa library database. Several references were also provided by DRDC staff and by partners. The principal author searched for and read references on CI, then recorded bibliographic and content information. In addition, the references were categorized and ordered based on some key characteristics.

Results: This publication is a documented literature search for CI in the context of public safety and security. It is a collection of approximately 200 references, comprising government publications, academic research, and reports produced by non-governmental or private sector organizations. The document provides bibliographic information, abstracts (when available), and content descriptions for each of the references. In addition, the references are presented in the following categories: national approaches to CI; processes for managing CI; incident case studies and lessons learned; business continuity; and miscellaneous references.

Significance: This document provides an extensive literature search in the area of CI. The references are categorized and ordered in a logical way that permits readers to quickly search and find references. The abstracts and descriptive information should allow readers to determine the relevance of the references to their work and/or interests while the bibliographic information facilitates location of references. Thus, the literature search document can be a resource for DRDC and external partners.

Future plans: At present, the electronic copies of the reference documents are stored on a CSS share drive. In the future, it could be valuable to create a database, which will facilitate more efficient searches through the references. As new material is published, the collection of reference documents should be updated and expanded.

Sommaire

Références relatives aux infrastructures essentielles : Recherche documentaire

Kyungryun (Cathy) Pak, Lynne Genik, Centre des sciences pour la sécurité de RDDC; DRDC CSS TN 2012-013; R & D pour la défense Canada – CSS; octobre 2012.

Contexte : Le projet de collaboration entre Emergency Management British Columbia (EMBC) et Recherche et développement pour la défense Canada (RDDC) vise à améliorer les capacités de gestion des urgences en appliquant une approche scientifique et en démontrant la valeur de celle-ci. Le projet porte principalement sur l'évaluation des risques (ER) et les infrastructures essentielles (IE), et les analyses documentaires dans ces deux domaines ont été effectuées lors de la phase initiale du projet. Cependant, RDDC a souligné la valeur potentielle d'examens plus exhaustifs. Par conséquent, des recherches documentaires approfondies ont été effectuées et documentées. Le présent document expose les résultats de la recherche documentaire sur les IE.

Méthode : La recherche documentaire a été effectuée principalement au moyen de bases de données en ligne comme la base de données de recherche de RDDC et la base de données de la bibliothèque de l'Université d'Ottawa. Plusieurs références ont également été fournies par le personnel de RDDC et des partenaires. L'auteure principale a cherché et lu des références sur les IE, puis a consigné les renseignements bibliographiques et les renseignements sur le contenu. De plus, les références ont été classées par catégories et ordonnées en fonction de certaines caractéristiques clés.

Résultats : Cette publication est une recherche documentaire sur les IE dans le contexte de la sûreté et de la sécurité publique. Il s'agit d'une collection d'environ 200références, qui comprennent des publications gouvernementales, de la recherche universitaire et des rapports d'organismes non gouvernementaux et du secteur privé. Le document fournit des renseignements bibliographiques, des résumés (s'il y a lieu) et des descriptions de contenu pour chacune des références. En outre, les références sont présentées dans les catégories suivantes : approches nationales aux IE; processus de gestion des IE; études de cas d'incident et leçons apprises; continuité des activités; références diverses.

Importance : Ce document présente une recherche documentaire approfondie dans le domaine des IE. Les références sont classées par catégories et ordonnées d'une façon logique qui permet aux lecteurs de chercher et de trouver rapidement les références. Les résumés et l'information descriptive devraient permettre aux lecteurs de déterminer la pertinence des références pour ce qui est de leur travail et de leurs intérêts, tandis que l'information bibliographique facilite le repérage des références. Par conséquent, le document de recherche documentaire peut servir de ressource pour RDDC et les partenaires externes.

Perspectives : À l'heure actuelle, les copies électroniques des documents de référence sont stockées dans un lecteur partagé du CSS. Dans l'avenir, il serait utile de créer une base de données qui favoriserait l'efficacité des recherches dans les références. À mesure que du nouveau matériel est publié, la collection des documents de référence devrait être mise à jour et élargie.

Table of contents

1 Introduction

1.1 Background

For the Vancouver 2010 Olympic and Paralympic Winter Games (V2010), Defence Research and Development Canada (DRDC) provided scientific support for Emergency Management British Columbia (EMBC). After V2010, EMBC and DRDC initiated a collaborative project with the aim of applying scientific practices to improve emergency management capabilities, focusing on the areas of risk assessment (RA) and critical infrastructure (CI).

In the initial phase of the project, DRDC worked on defining the problem and developed a solution strategy. During this process, a literature review was completed for RA and CI, and was documented in a DRDC Technical Memorandum[1]. However, DRDC identified the potential value of more comprehensive literature searches. As a result, the principal author, a co-op student, was engaged to conduct and document extensive literature searches on RA and CI.

1.2 Purpose

The purpose of this paper is to present a documented literature search for CI as it pertains to public safety and security. The literature search for RA is available in another document.

The intent of this document is not to provide an analytical review of the references included in the literature search. Instead, readers can use the organization and descriptions of the references to identify and acquire references that they find most valuable.

1.3 Scope

The literature search document provides references on CI in the context of public safety and security. It includes government publications, academic research, and the work of non-governmental or private sector organizations. The reference collection is mostly comprised of publications from developed countries such as Canada, the United States, the United Kingdom, Australia and Germany because of their applicability to Canadian society, as well as the accessibility of the references. All references included in this literature search are unclassified, although some are subject to limited distribution.

CI is a vast and complex field of work, and this document is not a comprehensive literature search of all existing references on CI. Rather, it presents a selection of approximately 200 references which were considered to be pertinent to Canadian public safety and security at the time of publication.

1.4 Methodology

This literature search was primarily conducted using online databases such as the DRDC research database and the University of Ottawa library database. In addition, several references were provided by DRDC staff and by partners.

The documentation of the literature search occurred in several phases. First, the principal author read through the references and recorded bibliographic information, abstracts, and key terms. In cases where abstracts were not available or did not sufficiently describe the content of the reference documents,

[1] See Reference 2.3.1.1

additional information was recorded. This included background information, purpose, goals, scope, audience, document descriptions, as well as key subject areas or sections.

The references were then categorized and further grouped as follows:

- National Approaches to CI: by the type and intent of the references. Sub-categories were further divided according to the country in which the references apply;
- Processes for Managing CI: by the six different components of the CI management process;
- Incident Case Studies and Lessons Learned: by the country in which the incident occurred;
- Business Continuity: by the type and intent of the references;
- Miscellaneous: contains no sub-sections.

This categorization scheme is illustrated in Figure 1.

Within each sub-section, similar references were grouped, then ordered from most to least recent in order to give precedence to the most current references.

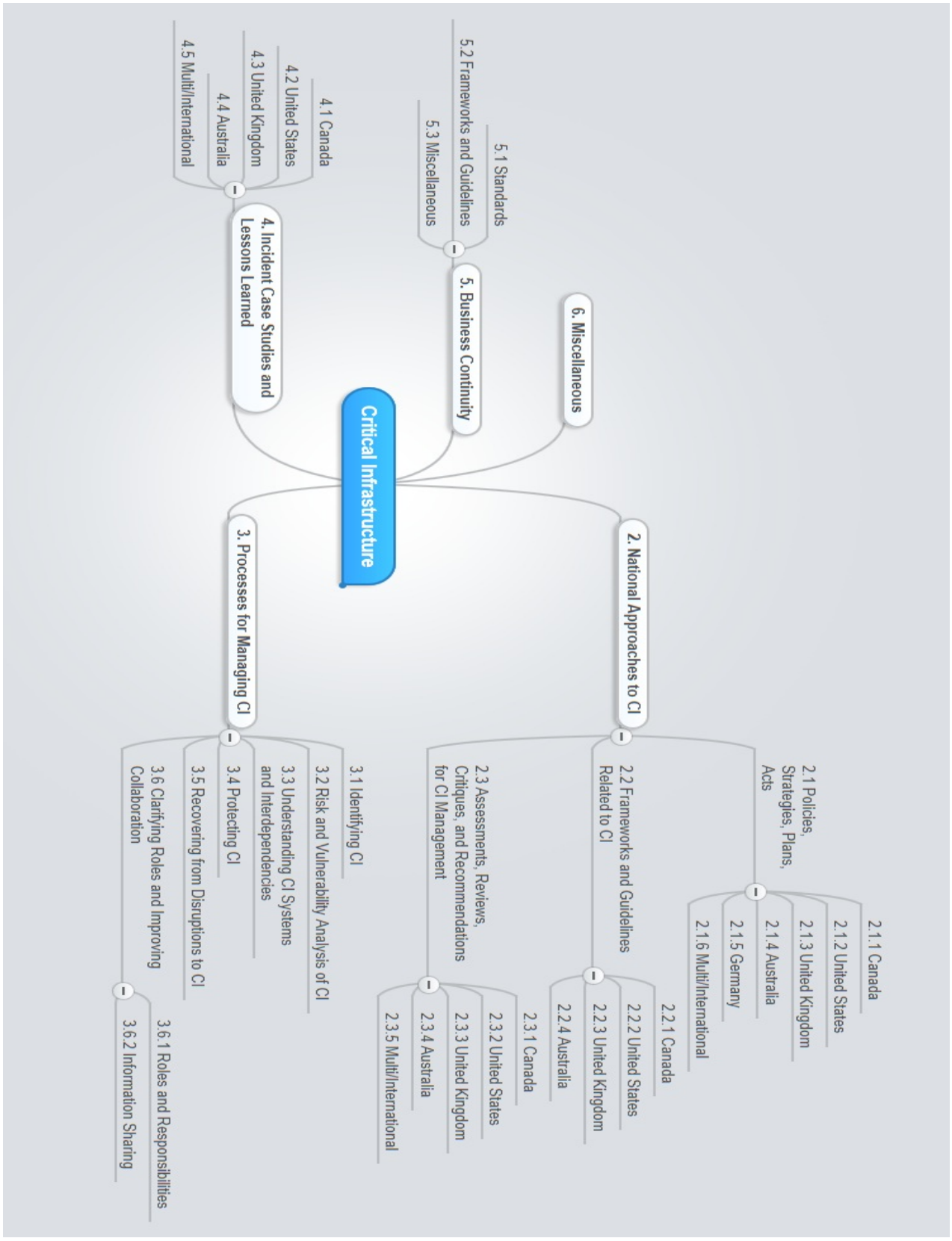

Figure 1- Categorization Scheme

1.5 Document Structure

This document is divided into seven chapters. This chapter provided introductory material. References which describe CI approaches in various countries are presented in the next chapter. Chapter 3 includes references which describe the approaches used for specific components of CI management. Incident case studies and lessons learned are presented in Chapter 4, and references on business continuity appear in Chapter 5. Lastly, Chapter 6 includes miscellaneous references, and a summary is provided in Chapter 7.

2 National Approaches to CI

Overview

This chapter presents references which reflect national approaches to critical infrastructure (CI) in several countries. These references are very high-level documents which describe general strategies and practices related to the countries' efforts in CI. Thus, references which describe a country's more detailed and methodical approaches to more specific components of CI management were not included in this chapter, but can be found in Chapter 3.

This chapter is divided into the following sections, and then further divided by country:

- Section 2.1: policies, strategies, plans, and acts which outline the governments' approach to managing CI.
    - Sub-categories: Canada; the United States; the United Kingdom; Australia; Germany; and Multi/International.
- Section 2.2: frameworks and guidelines related to CI.
    - Sub-categories: Canada; the United States; the United Kingdom; and Australia.
- Section 2.3: assessments of the countries' CI, as well as reviews, critiques, and recommendations for CI management.
    - Sub-categories: Canada; the United States; the United Kingdom; Australia; Multi/International

Within sub-sections, related or similar references are grouped, and then ordered chronologically from most to least recent.

Note: Some of the references included in this chapter are not national in scope. Rather, they are regional, or apply to certain sectors across several nations. However, these references were included in this chapter because they describe or present a high-level approach to critical infrastructure management.

2.1 Policies, Strategies, Plans, and Acts

2.1.1 Canada

2.1.1.1 National Strategy for Critical Infrastructure

Title: National Strategy for Critical Infrastructure
Author(s): Federal, Provincial and Territorial Governments of Canada
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Canada
Edition: N/A
Pages: 12
Retrieved from: Public Safety website
Hyperlink: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf
Date of Publication: 2009

Purpose:

- "To strengthen the resiliency of critical infrastructure in Canada. The Strategy works toward this goal by setting the direction for enhancing the resiliency of critical infrastructure against current and emerging hazards." [p. 3]

Strategic Objectives:

- "Build partnerships;
- Implement an all-hazards risk management approach; and
- Advance the timely sharing and protection of information among partners." [p. 3]

Description:

- "The National Strategy for Critical Infrastructure represents the first milestone in the road ahead. It identifies a clear set of goals and objectives and outlines the guiding principles that will underpin our efforts to strengthen the resiliency of critical infrastructure. The National Strategy establishes a framework for cooperation in which governments and owners and operators can work together to prevent, mitigate, prepare for, respond to, and recover from disruptions of critical infrastructure and thereby safeguard the foundations of our country and way of life." [p. 3]

2.1.1.2 Action Plan for Critical Infrastructure

Title: Action Plan for Critical Infrastructure
Author(s): Federal, Provincial and Territorial Governments of Canada
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Canada
Edition: Unavailable
Pages: 25
Retrieved from: Public Safety website
Hyperlink: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ct-pln-eng.pdf
Date of Publication: 2009

Description:

- This *Action Plan* is a supporting document to the *National Strategy for Critical Infrastructure.* These two documents establish a "collaborative federal, provincial, territorial and critical infrastructure sector approach that will be used to strengthen critical infrastructure resiliency." [p. 2]
- The Action Plan builds on the key elements of the National Strategy by outlining action items for those areas. They are:
    - Build Partnerships
    - Share and protect information
    - Implement an all-hazards risk management approach

2.1.1.3 In response to: Consultations on Working Towards a National Strategy and Action Plan for Critical Infrastructure

Title: In response to: Consultations on Working Towards a National Strategy and Action Plan for Critical Infrastructure
Author(s): Federation of Canadian Municipalities (FCM)
Organization: Federation of Canadian Municipalities (FCM)
Publisher: Federation of Canadian Municipalities (FCM)
Publishing Location: Ottawa, ON
Edition: Unavailable
Pages: 4
Retrieved from: Federation of Canadian Municipalities (FCM) website
Hyperlink:
http://www.fcm.ca/Documents/reports/Consultations_on_Working_Towards_a_National_Strategy_and_Action_Plan_for_Critical_Infrastructure_EN.pdf
Date of Publication: July 21, 2008

Background:

- This paper voices the Federation of Canadian Municipalities' response to the document, *Working Towards a Strategy and Action Plan for Critical Infrastructure.*

Description:

- This response paper highlights the critical role that municipal governments play in responding to emergencies, investing in and owning infrastructure, and providing the essential infrastructure and services needed to support economic growth.
- The authors claim that the proposed *Action Plan* does not sufficiently recognize municipalities as major players in critical infrastructure protection.
- In addition, the authors argue that municipal governments lack the financial resources that are needed to protect the critical infrastructure that lies in their boundaries.

Additional Information:
The Federation of Canadian Municipalities proposes 3 recommendations:
1)"Acknowledge municipalities as key partners in the Action Plan, in recognition of the fact that municipalities build, own and maintain the majority of Canada's publicly-held infrastructure.
2) Ensure municipal representation, either formally or informally, in the Federal/Provincial/Territorial Critical Infrastructure Working Group. At the very least, ensure formal municipal participation in the sector networks for energy and utilities, finance, transportation, government, water, and safety.
3) Increase funding to JEPP to meet the scale of the challenge of protecting critical structure in the new security environment." [p. 4]

2.1.1.4 Working Towards a National Strategy and Action Plan for Critical Infrastructure

Title: Working Towards a National Strategy and Action Plan for Critical Infrastructure
Author(s): Public Safety Canada
Organization: Public Safety Canada
Publisher: Public Safety Canada
Publishing Location: Canada
Edition: Unavailable
Pages: 38
Retrieved from: Canadian Water and Wastewater Association website
Hyperlink: http://www.cwwa.ca/pdf_files/CIPlan%20-%20may%202008.pdf
Date of Publication: 2008

Background:

- This document is a draft version of the *National Strategy for Critical Infrastructure* (2009), and the *Action Plan for Critical Infrastructure* (2009).
- The authors of this document asked the members of the critical infrastructure sectors to provide feedback in 2008.

Description:
This document contains two parts:

1) Part 1: Working Towards a National Strategy for Critical Infrastructure: Strategy
Purpose:

- "to strengthen the resiliency of critical infrastructure in Canada. The Strategy works toward this goal by setting the direction for enhancing the resiliency of Canada's critical infrastructure against current and emerging hazards." [p. 3]

Strategic Objectives:

- "build trusted and sustainable partnerships;
- implement an all-hazards risk management approach; and,
- advance the timely sharing and protection of information among partners" [p. 3]

Description:

- This Strategy describes the government of Canada's approach to achieving its three strategic objectives for Critical Infrastructure protection.

2) Part 2: Working Towards a National Strategy for Critical Infrastructure: Action Plan
Description:

- The *Action Plan* builds on the *National Strategy*, and "sets out action items in the areas of partnerships, risk management and information sharing." [p. 14]

2.1.1.5 Securing an Open Society: One Year Later - Progress Report on the Implementation of Canada's National Security Policy

Title: Securing an Open Society: One Year Later - Progress Report on the Implementation of Canada's National Security Policy
Author(s): Privy Council Office
Organization: Privy Council Office
Publisher: Privy Council Office
Publishing Location: Canada
Edition: N/A
Pages: 61
Retrieved from: Privy Council Office website
Hyperlink: http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/secure/secure-eng.pdf
Date of Publication: April 2005

Description:

- "The National Security Policy focuses attention and actions on building a more integrated security system and sets out specific actions in six key areas: intelligence, emergency planning and management, public health emergencies, transportation security, border security, and international security.
- Over the last year, significant progress has been made in implementing a number of initiatives identified in the National Security Policy, as well as several other national security enhancements." [p. ix]
- This document provides an overview of the key achievements in each of the six focus areas.

2.1.1.6 Securing an Open Society: Canada's National Security Policy

Title: Securing an Open Society: Canada's National Security Policy
Author(s): Privy Council Office
Organization: Privy Council Office
Publisher: Privy Council Office
Publishing Location: Canada
Edition: N/A
Pages: 60
Retrieved from: Government of Canada Publications website
Hyperlink: http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf
Date of Publication: April 2004

Description:

- "Securing an Open Society: Canada's National Security Policy is a strategic framework and action plan designed to ensure that Canada is prepared for and can respond to current and future threats. The focus is on events and circumstances that generally require a national response as they are beyond the capacity of individuals, communities or provinces to address alone." [p. vii]

Additional Information:

- "The National Security Policy also includes chapters on six key strategic areas. Each chapter builds on important steps already taken, addresses specific security gaps, and sets out the principles upon which the policy will be implemented and evolve." [p. viii] The chapters are:
  1. Canada's Approach to National Security
  2. Building an Integrated Security System
  3. Intelligence
  4. Emergency Planning and Management
  5. Public Health Emergencies
  6. Transportation Security
  7. Border Security
  8. International Security
- This *National Security Policy* identifies critical infrastructure protection as a high priority gap, and makes reference to the development of the Canadian *Critical Infrastructure Protection Strategy*.

2.1.1.7 Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection

Title: Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection
Author(s): Government of Canada
Organization: Government of Canada
Publisher: Government of Canada
Publishing Location: Canada
Edition: Unavailable
Pages:181
Retrieved from: Association of Canadian Port Authorities website
Hyperlink: http://www.acpa-ports.net/advocacy/pdfs/nscip_e.pdf
Date of Publication: November 2004

Purpose:

- "This paper presents the Government of Canada's position on the development of a comprehensive national approach to critical infrastructure protection (CIP). It is intended to elicit feedback from stakeholder groups and to form the basis of a national strategy for critical infrastructure protection." [p. 3]

Description:

- This paper describes each of the elements of Canada's *National Critical Infrastructure Protection Strategy*. In addition, it outlines the Government of Canada's position on how these elements can be integrated into improving critical infrastructure protection.

Additional Information:
The key elements of the *National Critical Infrastructure Protection Strategy* are:

- Guiding principles
- Risk management
- Information sharing
- Inventory of critical infrastructure assets
- Threats and warnings
- Critical infrastructure interdependencies
- Governance mechanisms
- Research and development

2.1.1.8 Ontario Critical Infrastructure Assurance Program

Title: Ontario Critical Infrastructure Assurance Program
Author(s): Emergency Management Ontario
Organization: Emergency Management Ontario
Publisher: Emergency Management Ontario
Publishing Location: Unavailable
Edition: Unavailable
Pages: 5
Retrieved from: Emergency Management Ontario website
Hyperlink:
http://www.emergencymanagementontario.ca/stellent/groups/public/@mcscs/@www/@emo/documents/abstract/ec157278.pdf
Date of Publication: Revised May 19, 2011

Aim and objectives:

- "The aim of the OCIAP [Ontario Critical Infrastructure Assurance Program] is to increase the resiliency of the province's critical infrastructure, so that it is more sustainable during an adverse event." [p. 3]

Description:

- This document is a strategic policy statement that outlines the components of the Ontario Critical Infrastructure Assurance Program.

Additional Information:

- This document includes sections on:
  - Vision
  - Background
  - Aim and objectives
  - Objectives
  - Definitions
  - Key Principles
  - Approach
  - Reporting Structure
  - Core Activities
- The four core activities that comprise the Ontario Critical Infrastructure Assurance Program are:
  1) "Form sector working groups...
  2) Identify and assess critical infrastructures - their dependencies and interdependencies...
  3) Identify assurance solutions to mitigate risks to critical infrastructure...
  4) Refine, enhance and promote best practice in critical infrastructure assurance" [p. 5]

Note: "This strategic policy statement is consistent with Emergency Management Ontario's *Emergency Management doctrine,* and with the *National Strategy and Action Plan for Critical Infrastructure"* [p. 5]

2.1.1.9 Access to Information Act (R.S.C., 1985, c. A-1)

Title: Access to Information Act (R.S.C., 1985, c. A-1)
Author(s): N/A
Organization: N/A
Publisher: Minister of Justice
Publishing Location: Canada
Edition: N/A
Pages: 70
Retrieved from: Department of Justice Canada website
Hyperlink: http://laws-lois.justice.gc.ca/PDF/A-1.pdf
Current to: June 27, 2012
Last amended: March 16, 2012

Overview:

- "An Act to extend the present laws of Canada that provide access to information under the control of the Government of Canada." [p. 1]

"Purpose:

> 2. (1) The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government." [Section 2.1, p. 1]

Additional Information:

- Section 8 of the *Emergency Management Act* has amended Subsection 20(1) of the *Access of Information Act* by adding paragraph (b.1).
- This amendment adds that any information provided by a third party under section 2 of *the Emergency Management Act* concerning the "vulnerability of the third party's buildings or other structures, its networks or systems" [subsection 20(1) (b.1), p. 19] or its methods of protection, shall not be disclosed by the head of a government institution.
- Related amendments of the *Access to Information Act* apply to subsection 20(6), 27(1) and 35(2).

Note: This supplementary information was provided by the Treasury Board Secretariat website, at http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/2007-08-in-ai-eng.asp

2.1.1.10 Emergency Management Act (S.C. 2007, c. 15)

Title: Emergency Management Act (S.C. 2007, c. 15)
Author(s): N/A
Organization: N/A
Publisher: Minister of Justice
Publishing Location: Canada
Edition: N/A
Pages: 8
Retrieved from: Department of Justice Canada website
Hyperlink: http://laws-lois.justice.gc.ca/PDF/E-4.56.pdf
Current to: June 27, 2012
Last amended: August 3, 2007

Overview:

- "An Act to provide for emergency management and to amend and repeal certain Acts." [p. 1]

Description:

- This Act provides definitions and prescribes the responsibilities of the Minister of Public Safety and Emergency Preparedness, other Ministers' responsibilities for emergency management, and the orders or regulations which may be made on the recommendation of the Minister.

2.1.1.11 Privacy Act (R.S.C., 1985, c. P-21)

Title: Privacy Act (R.S.C., 1985, c. P-21)
Author(s): N/A
Organization: N/A
Publisher: Minister of Justice
Publishing Location: Canada
Edition: N/A
Pages: 62
Retrieved from: Department of Justice Canada website
Hyperlink: http://laws-lois.justice.gc.ca/PDF/P-21.pdf
Current to: June 27, 2012
Last amended: March 16, 2012

Overview:

- "An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves." [p. 1]

Purpose:

> "2. The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.
> 1980-81-82-83, c. 111, Sch. II “2”." [Section 2, p. 1]

2.1.1.12 Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

Title: Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)
Author(s): N/A
Organization: N/A
Publisher: Minister of Justice
Publishing Location: Canada
Edition: N/A
Pages: 53
Retrieved from: Department of Justice Canada website
Hyperlink: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf
Current to: June 27, 2012
Last amended: April 1, 2011

Overview:

- "An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act." [p. 1]

"Purpose:

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." [Section 3, p. 3]

"Application:

4. (1) This Part applies to every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of commercial activities; or
(b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Limit:

(2) This Part does not apply to
(a) any government institution to which the Privacy Act applies;
(b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or
(c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose." [Section 4, p. 4]

2.1.1.13 Department of Public Safety and Emergency Preparedness Act (S.C. 2005, c. 10)

Title: Department of Public Safety and Emergency Preparedness Act (S.C. 2005, c. 10)
Author(s): N/A
Organization: N/A
Publisher: Minister of Justice
Publishing Location: Canada
Edition: N/A
Pages: 10
Retrieved from: Department of Justice Canada website
Hyperlink: http://laws-lois.justice.gc.ca/PDF/P-31.55.pdf
Current to: June 27, 2012
Last amended: August 3, 2007

Overview:

- "An Act to establish the Department of Public Safety and Emergency Preparedness and to amend or repeal certain Acts." [p. 1]

Description:

- This Act establishes the Department of Public Safety and Emergency Preparedness. It also prescribes the powers, duties and functions of the Minister as well as the transitional provisions.

2.1.2 United States

2.1.2.1 National Infrastructure Protection Plan - Partnering to Enhance Protection and Resiliency

Title: National Infrastructure Protection Plan - Partnering to Enhance Protection and Resiliency
Author(s): Department of Homeland Security
Organization: Department of Homeland Security
Publisher: Unavailable
Publishing Location: United States of America
Edition: Unavailable
Pages: 188
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
Date of Publication: 2009

Goal:

- "The overarching goal of the National Infrastructure Protection Plan (NIPP) is to:
  Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nations' CIKR [Critical Infrastructure and Key Resources] and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency." [p. 1]

Description:

- "Together, the NIPP and SSPs [Sector-Specific Plans] provide the mechanisms for: identifying critical assets, systems, and networks, and their associated functions; understanding threats to CIKR; identifying and assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and enhancing information-sharing mechanisms and protection and resiliency within and across CIKR sectors." [p. 8]

Scope:

- "The NIPP considers a full range of physical, cyber, and human risk elements within and across sectors." [p. 9] However, there is a special focus on terrorist attacks.

Applicability:

- A wide array of public and private sector CIKR partners

Additional Information:
The NIPP provides information on the components and processes that will form and implement the national approach to protecting CIKR. They are:

- Authorities, Roles, and Responsibilities
- The Strategy: Managing risk
  (Includes the NIPP's risk management framework)
- Organizing and Partnering for CIKR Protection
- CIKR Protection as Part of the Homeland Security Mission
- Ensuring an Effective, Efficient Program Over the Long Term
- Providing Resources for the CIKR Protection program

2.1.2.2 Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection

Title: Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection
Author(s): Issued by George W. Bush
Organization: N/A
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: N/A
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1
Date of Publication: December 17, 2003

Abstract:
"Homeland Security Presidential Directive 7 establishes a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The directive defines relevant terms and delivers 31 policy statements. These policy statements define what the directive covers and the roles various federal, state, and local agencies will play in carrying it out"[2].

Purpose:
- "This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks"[3].

Additional Information:
This document includes the following sections:
- Definitions
- Policy
- Roles and Responsibilities of the Secretary
- Roles and Responsibilities of Sector-Specific Federal Agencies
  - Designates Sector-specific agencies to infrastructure sectors
- Roles and Responsibilities of Other Departments, Agencies, and Offices
- Coordination with the Private Sector
- National Special Security Events
- Implementation
  - Requires the Secretary to produce a "comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection"[4].

[2] From http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1
[3] Ibid.
[4] Ibid.

2.1.2.3 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

Title: The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
Author(s): Unavailable
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 96
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf
Date of Publication: February 2003

Strategic objectives of the *Strategy:*

1. "To identify and assure the protection of those assets, systems, and functions that we deem most "critical" in terms of national-level public health and safety, governance, economic and national security, and public confidence." [p. 2]
2. "To assure the protection of infrastructures and assets that face a specific, imminent threat." [p. 2]
3. "To pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time." [p. 3]

Description:

- "This document defines the road ahead for a core mission area identified in the President's National Strategy for Homeland Security - reducing the Nation's vulnerability to acts of terrorism by protecting our critical infrastructures and key assets from physical attack.
- This document...identifies a clear set of national goals and objectives and outlines the guiding principles that will underpin our efforts to secure the infrastructures and assets vital to our national security, governance, public health and safety, economy and public confidence.
- This *Strategy* also provides a unifying organization and identifies specific initiatives to drive our near-term national protection priorities and inform the resource allocation process. Most importantly, it establishes a foundation for building and fostering the cooperative environment in which government, industry, and private citizens can carry out their respective protection responsibilities more effectively and efficiently…
- This document provides direction to the federal departments and agencies that have a role in critical infrastructure and key asset protection. It also suggests steps that state and local governments, private sector entities, and concerned citizens across America can take to enhance our collective infrastructure and asset security." [p. vii]

Additional Information:
This Strategy covers the following areas:

- "The Case for Action
- National Policy and Guiding Principles
- Organizing and Partnering for Critical Infrastructure and Key Asset Protection
- Cross-Sector Security Priorities
- Securing Critical Infrastructures
- Protecting Key Assets
- Conclusion" [p. v]

2.1.2.4 National Infrastructure Protection Plan - International Issues for CI/KR Protection

Title: National Infrastructure Protection Plan - International Issues for CI/KR Protection
Author(s): Department of Homeland Security (DHS)
Organization: Department of Homeland Security (DHS)
Publisher: Department of Homeland Security (DHS)
Publishing Location: Unavailable
Edition: Unavailable
Pages: 2
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf
Date of Publication: Unavailable

Description:

- This document provides a brief overview of the international issues which arise in the protection of critical infrastructure and key resources (CIKR).
- In addition, it describes examples of existing agreements for international coordination for CIKR protection.

2.1.2.5 Banking and Finance: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

Title: Banking and Finance: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan
Author(s): Department of the Treasury in close collaboration with the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC)
Organization: Department of the Treasury and the U.S. Department of Homeland Security (DHS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 1st ed.
Pages: 116
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf
Date of Publication: May 2007

Background:

- "Working through this public-private partnership, the Department of the Treasury, as the Sector-Specific Agency (SSA) for the Banking and Finance Sector, has developed this Sector-Specific Plan (SSP) in close collaboration with the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC).
- This SSP, along with the SSPs from the 16 other critical infrastructures identified in Homeland Security Presidential Directive 7 (HSPD-7), are part of the overall National Infrastructure Protection Plan (NIPP)." [p. 1]

Description:

- "This SSP contains the Banking and Finance Sector's strategy for working collaboratively with public and private sector partners to identify, prioritize, and coordinate the protection of critical infrastructure. This SSP also summarizes the extensive activities the sector has undertaken already to reduce vulnerabilities and share information." [p. 1]

Additional Information:

- This SSP is structured in alignment with the NIPP's risk management framework and includes other sector responsibilities. The sections are:

1. Sector Profile and Goals
2. Identify Assets, Systems, Networks, and Functions
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs
6. Measure Progress
7. CI/KR Protection R&D
8. Manage and Coordinate SSA Responsibilities

2.1.2.6 Chemical Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Chemical Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): Chemical Sector-Specific Agency
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 143
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-chemical-2010.pdf
Date of Publication: 2010

Description:

- "The Chemical Sector-Specific Plan provides the unifying structure for the integration of Chemical Sector protection efforts into a single national program to help achieve the goal of a safe, secure, and resilient America through enhanced protection of the Nation's critical infrastructure and key resources (CIKR).
- As an annex to the National Infrastructure Protection Plan (NIPP), the Chemical Sector-Specific Plan describes how the NIPP risk management framework is being implemented in and integrated with both the voluntary programs already underway in the Chemical Sector and the promulgated regulatory standards for chemical facility security." [p. i]

Additional Information:
This SSP conforms to the NIPP's risk management framework, and is structured in alignment with its elements and other sector responsibilities. The sections are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating SSA [Sector-Specific Agency] Responsibilities

2.1.2.7 Commercial Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Commercial Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): Commercial Facilities Sector Specific Agency
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 174
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf
Date of Publication: 2010

Background:

- "The Commercial Facilities (CF) Sector-Specific Plan (SSP) was created to complement the National Infrastructure Protection Plan (NIPP) by developing efforts to improve the protection of the CF Sector in an all-hazards environment." [p. 1]

Description:

- "The CF-SSP establishes a relationship between the government and the private sector to foster the cooperation necessary to improve the protection of the sector from natural or manmade disasters.
- The CF-SSP sets a path forward for the sector to collectively identify and prioritize assets, assess risk, implement protective programs, and measure the effectiveness of protective programs.
- The CF-SSP reflects the collaborative efforts between government and private sector stakeholders who are dedicated to the protection of key resources within the CF Sector." [p. 1]

Additional Information:
This SSP is structured in alignment with the NIPP's risk management framework and other sector responsibilities. The chapters are:

1. Sector Profile and Goals
2. Identify Assets, Systems, Networks, and Functions
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CI/KR Protection Research and Development
8. Manage and Coordinate Sector-Specific Agency Responsibilities

2.1.2.8 Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): U.S. Department of Homeland Security's National Communications System (NCS)
Organization: U.S. Department of Homeland Security's National Communications System (NCS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 126
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf
Date of Publication: 2010

Purpose:

- "This plan is intended to enhance the Nation's communications infrastructure protection framework through collaboration of public and private sector partners.
- For government partners, the processes outlined in this plan support their missions to execute, command, control, and coordination; to provide national, economic, and homeland security; and to ensure public health and safety.
- For private sector partners, enhanced security and critical infrastructure protection are crucial for safeguarding physical, cyber, and human assets, systems, and networks; ensuring continuity of business operations; and enhancing shareholder value. [p. 7-8]

Scope:

- "The CSSP [Communications Sector-Specific Plan] reflects the scope of the Communications Sector's risk management process as outlined by the NIPP. This plan outlines the infrastructure protection activities—physical, cyber, and human—through which the Communications Sector industry and government partners will individually and cooperatively mitigate risks to critical national communications infrastructure assets and services." [p. 8]

Description:

- "The CSSP focuses the Communications Sector's risk management process on identifying and protecting nationally critical architecture elements; ensuring overall network reliability; maintaining "always-on" services for critical customers; and quickly restoring critical communications functions and services following a disruption." [p. 3]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in support of the NIPP risk management framework and other sector responsibilities. They are:

1. Establish Sector Goals and Objectives
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. Coordinate CIKR Protection R&D Efforts
8. Manage and Coordinate SSA Responsibilities

2.1.2.9 Critical Manufacturing Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Critical Manufacturing Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): U.S. Department of Homeland Security (DHS) and Critical Manufacturing Sector partners
Organization: U.S. Department of Homeland Security (DHS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 1st ed.
Pages: 72
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-critical-manufacturing-2010.pdf
Date of Publication: 2010

Description:

- "The SSP provides the unifying structure for the integration of Critical Manufacturing Sector protection efforts into a single national program to help achieve the goal of a safer, more resilient infrastructure.
- An annex to the National Infrastructure Protection Plan (NIPP), the SSP describes how the NIPP risk management framework—the six-step process for managing the risks associated with protecting the Nation's critical infrastructure and key resources (CIKR)—is being implemented and integrated with voluntary programs already underway in the Critical Manufacturing Sector." [p. 1]

Additional Information:
This SSP is structured in alignment with the NIPP's risk management framework and other sector responsibilities. The chapters are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks (Consequences, Vulnerabilities, and Threats)
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resiliency Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.10 Dams Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Dams Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): Unavailable
Organization: U.S. Department of Homeland Security (DHS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 136
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-dams-2010.pdf
Date of Publication: 2010

Background:

- "The Dams Sector-Specific Plan (DSSP) was developed to complement the National Infrastructure Protection Plan (NIPP) in achieving a safer, more secure, and more resilient Dams Sector by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks, natural disasters, and other incidents." [p. 1]

Description:

- "The DSSP portrays the collaborative partnership among all levels of government and the private sector that fosters the cooperation necessary to improve the protection and resilience of the Dams Sector. This plan describes the sector-wide processes required to identify and prioritize assets, assess risk in the sector, implement protective programs and resilience strategies, and measure their effectiveness." [p. 1]

Additional Information:
This SSP is structured in alignment with the NIPP's risk management framework and other sector responsibilities. The chapters are:

1. Dams Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.11 Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): Department of Defense (DoD)
Organization: Department of Defense (DoD) and the U.S. Department of Homeland Security (DHS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition Unavailable
Pages: 105
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf
Date of Publication: 2010

Background:

- "The President, in Homeland Security Presidential Directive 7 (HSPD-7), designated the Department of Defense (DoD) as the Sector-Specific Agency (SSA) responsible for leading a collaborative, coordinated effort to identify, assess, and improve the risk management of critical infrastructure within the Defense Industrial Base (DIB).
- In HSPD-7, the President also directed DoD to produce the DIB Sector-Specific Plan (SSP) in collaboration with private sector and interagency partners…
- This DIB SSP outlines the DoD approach to executing its SSA responsibilities." [p. 1]

Description:

- "The DIB SSP has taken on a more partnership-oriented approach to describe the status of DIB protection efforts, and outlines the sector vision, goals, objectives, risk assessment methodology, and comprehensive plan to implement tactical-level processes that lead to improved protection and resilience of DIB assets." [p. 11]

Additional Information:
This SSP aligns with the NIPP's risk management framework, and is structured according to its elements and other sector responsibilities. The chapters are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Responsibilities

2.1.2.12 Education Facilities Sector-Specific Plan: An Annex to the Government Facilities Sector-Specific Plan

Title: Education Facilities Sector-Specific Plan: An Annex to the Government Facilities Sector-Specific Plan
Author(s): Department of Education's (ED) Office of Safe and Drug-Free Schools (OSDFS)
Organization: Department of Education (ED) and the U.S. Department of Homeland Security (DHS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition Unavailable
Pages: 72
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf
Date of Publication: 2010

Background:

- "The Education Facilities Subsector (EFS) is a GFS [Government Facilities Sector] subsector under the National Infrastructure Protection Plan (NIPP) for coordinating infrastructure protection efforts for schools and higher education institutions.
- The U.S. Department of Education's (ED) Office of Safe and Drug-Free Schools (OSDFS) serves as the Sector-Specific Agency (SSA) for the subsector under the NIPP, as designated by the U.S. Department of Homeland Security (DHS)." [p. 1]

Description:

- "Consistent with specific DHS guidance, the 2010 EFS SSP addresses key changes to the 2009 NIPP (e.g., all-hazards approaches and an emphasis on resilience), describing the EFS vision and goal in terms of these changes and as they relate to protective efforts and associated metrics.
- The SSP also provides an overview of the education facilities profile, assets, risk assessment, prioritization, protective programs and resilience strategies, metrics, research and development (R&D), and subsector management." [p. 3]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in support of the NIPP risk management framework and other sector responsibilities. They are:

1. Subsector Profile and Goal
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.13 Emergency Services Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Emergency Services Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): Unavailable
Organization: U.S. Department of Homeland Security (DHS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 128
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf
Date of Publication: 2010

Description:

- "The Emergency Services Sector-Specific Plan (SSP) is an annex to the National Infrastructure Protection Plan (NIPP) and addresses efforts to improve protection of the ESS in an all-hazards environment.
- The SSP establishes relationships among various government partners at all levels, and between the government and the private sector, to foster the cooperation necessary to improve protection of the sector from natural or manmade disasters.
- The SSP sets a path forward for the sector to collectively identify and prioritize its facilities and systems, assess risk, implement CIKR protective programs, and measure program effectiveness.
- This document reflects the collaborative efforts among all of the sector partners that are dedicated to protection of CIKR within the ESS." [p. 1]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in support of the NIPP risk management framework and other sector responsibilities. They are:

1. Sector Profile, Sector Partners, and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks (Consequences, Vulnerabilities, and Threats)
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating Sector-Specific Agency Responsibilities

2.1.2.14 Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): United States Department of Energy
Organization: U.S. Department of Homeland Security (DHS) and the United States Department of Energy
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 124
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf
Date of Publication: 2010

Background:

- The U.S. Department of Energy (DOE) has been designated the Sector-Specific Agency (SSA) for the Energy Sector, and is tasked with coordinating preparation and implementation of an Energy Sector-Specific Plan (SSP) that is an annex to the NIPP [National Infrastructure Protection Plan]." [p. 1]

Description:

- "Through the Energy SSP process, government and industry have established unprecedented cooperation and close partnership to develop and implement a national effort that brings together all levels of government, industry, and international partners. This updated 2010 Energy SSP is a reflection of that partnership and the achievements of the sector over the last three years." [p. 5]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in support of the NIPP risk management framework and other sector responsibilities. They are:

1. Sector Profile, Vision, and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection R&D
8. Managing and Coordinating SSA Responsibilities

2.1.2.15 Food and Agriculture Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Food and Agriculture Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): United States Department of Agriculture (USDA) and Department of Health and Human Services/Food and Drug Administration (HHS/FDA)
Organization: U.S. Department of Homeland Security (DHS), United States Department of Agriculture (USDA), and Department of Health and Human Services/Food and Drug Administration (HHS/FDA)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 184
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf
Date of Publication: 2010

Background:

- "The United States Department of Agriculture (USDA) and Department of Health and Human Services/Food and Drug Administration (HHS/FDA) are designated as Sector-Specific Agencies (SSAs) for the Food and Agriculture (FA) Sector by Homeland Security Presidential Directive 7 (HSPD-7)." [p. 5]

Description:

- "This document presents a strategic overview of the methods, programs, and activities that the FA Sector uses to continuously enhance CIKR protection efforts in the sector." [p. 7]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in support of the NIPP risk management framework and other sector responsibilities. They are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resiliency Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.16 Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): U.S. Department of Health and Human Services
Organization: U.S. Department of Homeland Security (DHS) and the U.S. Department of Health and Human Services
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 72
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf
Date of Publication: 2010

Background:

- "The U.S. Department of Health and Human Services (HHS) is the designated SSA [Sector-Specific Agency] for the Healthcare and Public Health (HPH) Sector. As the SSA, HHS is responsible for working with its sector partners to develop and maintain a Sector-Specific Plan (SSP) that details the application of the NIPP [National Infrastructure Protection Plan] risk management framework to the unique characteristics and risk landscape of the HPH Sector." [p. 8]

Description:

- "The Healthcare and Public Health (HPH) Sector-Specific Plan (SSP) complements the National Infrastructure Protection Plan (NIPP) by detailing the application of the NIPP framework to the unique characteristics and risk landscape of the sector.
- The SSP lays out a collaborative process among government and private sector partners to protect the HPH Sector from natural disasters, pandemics, terrorist attacks, and other manmade disasters, referred to collectively as “all hazards.”
- The plan describes current processes and sets a path forward for the sector to cooperatively identify and prioritize its assets, assess risk, implement protective programs, and measure the effectiveness of its protective programs. It summarizes research and development (R&D) activities in the sector and describes the sector’s approach to managing its responsibilities in the areas of partnership, training and education, and information sharing and protection." [p. 1]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in support of the NIPP risk management framework and other sector responsibilities. They are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection Research & Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.17 National Monuments and Icons Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: National Monuments and Icons Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): U.S. Department of the Interior (DOI)
Organization: U.S. Department of Homeland Security (DHS) and the U.S. Department of the Interior (DOI)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 64
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf
Date of Publication: 2010

Background:

- "The Department of the Interior (DOI), as the Sector-Specific Agency (SSA) for the National Monuments and Icons (NMI) Sector, is responsible for developing and updating the SSP for this sector." [p. 5]

Description:

- "The National Monuments and Icons (NMI) Sector-Specific Plan (SSP) was created to complement the National Infrastructure Protection Plan (NIPP) in improving protection of the NMI Sector in an all-hazard environment. The NMI SSP promotes a collaborative partnership at all levels of government to foster the cooperation necessary to improve the protection of NMI critical infrastructure and key resources (CIKR).
- The NMI SSP is a pathway to identify and prioritize assets, assess risk, implement protective programs, and measure the effectiveness of protective programs. This document represents the collaborative efforts of our sector partners, all dedicated to the protection and resilience of CIKR assets as it relates to all hazards within the NMI Sector." [p. 1]

Additional Information:
This plan is divided into 8 sections, in accordance with the elements of the NIPP's risk management framework and other sector-related functions. They are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resilience Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.18 Nuclear Reactors, Materials, and Waste Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Nuclear Reactors, Materials, and Waste Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): U.S. Department of Homeland Security (DHS)
Organization: U.S. Department of Homeland Security (DHS)
Publisher: U.S. Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 142
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-nuclear-2010.pdf
Date of Publication: 2010

Background:
- "The SSA [Sector Specific Agency] for the Nuclear Reactors, Materials, and Waste Sector is the U.S. Department of Homeland Security (DHS)." [p. 1]

Purpose:
- "The purpose of this document is to describe at the unclassified, unrestricted level the efforts through which Nuclear Sector assets, systems, and networks are protected." [p. 9]

Scope:
- "Homeland Security Presidential Directive 7 (HSPD-7) directs protection of commercial nuclear reactors used for generating electrical power and non-power reactors used for research, testing, and training; nuclear material in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and transportation, storage, and disposal of nuclear materials and waste.
- In accordance with the NIPP and the guidance published by the DHS NIPP Program Management Office, this SSP is focused on protecting the Nuclear Sector from a terrorist attack, while supporting an all-hazards approach in the context of other events." [p. 9]

Description:
- "The Nuclear SSP provides a detailed description of: specific processes used to identify, assess, prioritize, and protect Nuclear Sector CIKR; processes used to measure effectiveness; the approach required to implement protective activities, including descriptions of projects, initiatives, activities, periods, milestones, and resources." [p. 8-9]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in accordance with the NIPP's risk management framework and other sector responsibilities. They are:
1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protective Programs and Resiliency Strategies
6. Measure Effectiveness
7. CIKR Protection Research and Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.19 Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): Transportation Security Administration (TSA) and the United States Coast Guard (USCG)
Organization: U.S. Department of Homeland Security, Transportation Security Administration (TSA) and the United States Coast Guard (USCG)
Publisher: U.S. Department of Homeland Security
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 346
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation-systems-2010.pdf
Date of Publication: 2010

Background:

- "The Secretary of Homeland Security designated the Transportation Security Administration (TSA) and the United States Coast Guard (USCG) as the SSAs for the Transportation Systems Sector. The SSAs, in collaboration with the Department of Transportation (DOT) and other Federal, State, local, tribal, territorial, and private industry partners, share the responsibility for developing, implementing, and updating the SSP." [p. 13]

Description:

- "The Transportation Systems SSP describes collaboratively developed strategies to reduce risks to critical transportation infrastructure from the broad range of known and unknown terrorism threats. These threats span a multitude of scenarios from lone actors with explosives devices to complex and coordinated assaults such as the 9/11 attack or, potentially, attacks involving weapons of mass destruction.
- The SSP establishes the strategic goals and objectives to be implemented in order to achieve a shared vision of a safe and secure national transportation system and it explains processes and mechanisms to manage sector risks." [p. 1]

Additional Information:
This Sector-Specific Plan is divided into eight chapters, in alignment with the NIPP's risk management framework and other sector responsibilities. They are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Focus Areas
5. Develop and Implement Protective Programs and Resiliency Strategies
6. Measure Effectiveness
7. Research and Development
8. Managing and Coordinating SSA Responsibilities

2.1.2.20 Water Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan

Title: Water Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan
Author(s): United States Environmental Protection Agency (EPA)
Organization: U.S. Department of Homeland Security, U.S. Environmental Protection Agency
Publisher: U.S. Department of Homeland Security
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 88
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp-ssp-water-2010.pdf
Date of Publication: 2010

Background:

- "Homeland Security Presidential Directive 7 designates the U.S. Environmental Protection Agency (EPA) as the Federal lead for coordinating and assisting in protecting the Nation's critical Water Sector infrastructure." [p. 1]

Description:

- "The 2010 Water Sector-Specific Plan addresses risk-based critical infrastructure protection strategies for drinking water and wastewater utilities, regulatory primacy agencies, and an array of technical assistance partners. The Plan describes processes and activities to enable the protection, and increased resilience, of the sector's infrastructure." [p. i]

Additional Information:
This Sector-Specific Plan conforms to the NIPP's risk management framework. The plan is structured according to the elements of the framework, as well as other sector responsibilities. The chapters are:

1. Sector Profile and Goals
2. Identify Assets, Systems, and Networks
3. Assess Risks
4. Prioritize Infrastructure
5. Develop and Implement Protection Initiatives and Resilience Strategies
6. Measure Progress
7. CIKR Protection Research and Development
8. Managing and Coordinating Sector-Specific Agency Responsibilities

2.1.2.21 Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges

Title: Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges
Author(s): N. Eric Weiss (Specialist in Financial Economics)
Organization: Congressional Research Service (CRS)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 16
Retrieved from: Congressional Research Service (CRS) Report for Congress, from the Federation of American Scientists website
Hyperlink: http://www.fas.org/sgp/crs/misc/RL31873.pdf
Date of Publication: May 4, 2009

Description:

- "This report outlines the financial sector's recovery plans for two kinds of disasters: the inability to conduct transactions and large losses of asset value." [Summary]

Additional Information:
This report covers the following topics:

- Banking and Financial Institutions Form a Critical Infrastructure
- Pandemic Flu
- The Role of DHS
- Safety Net Measures in Place
- Safety and Continuity in Recent Experience
- Financial Business Continuity Initiatives
- Executive Branch Initiatives
- Legislation and Oversight
- Conclusion: Convergence of Public-Private Practices for Financial Continuity

2.1.2.22 Critical Infrastructures: Background, Policy and Implementation

Title: Critical Infrastructures: Background, Policy and Implementation
Author(s): John D. Moteff (Specialist in Science and Technology Policy)
Organization: Congressional Research Service (CRS)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 42
Retrieved from: CRS Report for Congress, retrieved from the Federation of American Scientists (FAS) website
Hyperlink: http://www.fas.org/sgp/crs/homesec/RL30153.pdf
Date of Publication: July 11, 2011

Description:

- "This report discusses in more detail the evolution of a national critical infrastructure policy and the institutional structures established to implement it. The report highlights five issues of Congressional concern: identifying critical assets; assessing vulnerabilities and risks; allocating resources; information sharing; and regulation. This report will be updated." [Summary]

Additional Information:
This report discusses the following:

- Federal Critical Infrastructure Protection Policy: In Brief
- The President's Commission on Critical Infrastructure Protection
- Presidential Decision Directive No. 63
- Restructuring by the Bush Administration
- The Obama Administration
- Department of Homeland Security
- Policy Implementation
- Issues and Discussion

2.1.2.23 Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience

Title: Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 48
Retrieved from: GAO-10-296, Report to Congressional Requesters
Hyperlink: http://www.gao.gov/assets/310/301494.pdf
Date of Publication: March 2010

"Why GAO Did this study

- According to the Department of Homeland Security (DHS), there are thousands of facilities in the United States that if destroyed by a disaster could cause casualties, economic losses, or disruptions to national security. The Homeland Security Act of 2002 gave DHS responsibility for leading and coordinating the nation's effort to protect critical infrastructure and key resources (CIKR). Homeland Security Presidential Directive 7 (HSPD-7) defined responsibilities for DHS and certain federal agencies—known as sector-specific agencies (SSAs)—that represent 18 industry sectors, such as energy. In accordance with the Homeland Security Act and HSPD-7, DHS issued the National Infrastructure Protection Plan (NIPP) in June 2006 to provide the approach for integrating the nation's CIKR.
- GAO was asked to study DHS's January 2009 revisions to the NIPP in light of a debate over whether DHS has emphasized protection—to deter threats, mitigate vulnerabilities, or minimize the consequences of disasters---rather than resilience---to resist, absorb, or successfully adapt, respond to, or recover from disasters.
- This report discusses (1) how the 2009 NIPP changed compared to the 2006 NIPP and (2) how DHS and SSAs addressed resiliency as part of their planning efforts. GAO compared the 2006 and 2009 NIPPs, analyzed documents, including NIPP Implementation Guides and sector-specific plans, and interviewed DHS and SSA officials from all 18 sectors about their process to identify potential revisions to the NIPP and address resiliency." [Introductory Page]

2.1.3 United Kingdom

2.1.3.1 A Summary of the: Sector Resilience Plans for Critical Infrastructure 2010/2011

Title: A Summary of the: Sector Resilience Plans for Critical Infrastructure 2010/2011
Author(s): Cabinet Office
Organization: Cabinet Office
Publisher: Cabinet Office
Publishing Location: London, UK
Edition: Unavailable
Pages: 42
Retrieved from: Cabinet Office website
Hyperlink: http://www.cabinetoffice.gov.uk/sites/default/files/resources/sector-resilience-plan-2011.pdf
Date of Publication: May 2011

Background:

- "In support of the National Security Strategy and the Strategic Defence and Security Review, the Critical Infrastructure Resilience Programme, led by the Cabinet Office, is developing a systematic, coordinated, cross-sector campaign to reduce the disruption caused by natural hazards to the UK's critical infrastructure.
- A key output from this programme are the Sector Resilience Plans, developed by lead government departments for the nine national infrastructure sectors setting out the current level of resilience of critical infrastructure to natural hazards." [p. 4]

Scope:

- The plans summarized in this document focus on the United Kingdom as a whole. However, separate arrangements exist within the Devolved Administrations.
- The plans reflect the resilience of the UK's critical infrastructure from natural hazard disruptions in the first quarter of 2011.

Description:

- This document provides a summary of sector plans for the United Kingdom's nine critical infrastructure sectors. These plans provide "a concise snapshot of each sector's resilience to natural hazards and outlines the approach sectors will take to improve the current level of resilience." [p. 5]

Additional Information:
For each of the nine plans that are summarized, this document provides:

- Overview
- Sector Approach
- Assessment of Existing Vulnerability
- Building resilience
- Background

2.1.3.2 Sector Resilience Plan for Critical Infrastructure 2010

Title: Sector Resilience Plan for Critical Infrastructure 2010
Author(s): Cabinet Office
Organization: Cabinet Office
Publisher: Cabinet Office
Publishing Location: London, UK
Edition: N/A
Pages: 33
Retrieved from: UK Government, National Archives website
Hyperlink:
http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/349100/sector-resilience-plan.pdf
Date of Publication: March 2010

Background:

- "The independent review by Sir Michael Pitt of the summer 2007 floods recommended the development of plans to reduce the vulnerability of critical national infrastructure to flooding and other natural hazards.
- Accordingly, the Government has established a Critical Infrastructure Resilience Programme: a collaboration between owners/operators of critical infrastructure in the nine recognised infrastructure sectors, government departments sponsoring these sectors, and regulators.
- A key output from this programme is the development of sector resilience plans, setting out the current level of resilience of critical infrastructure and essential services to natural hazards. The first iteration of the plans were completed at the end of 2009. They focussed on the resilience of the most critical infrastructure in each infrastructure sector, and to flooding only. Information in respect of other critical infrastructure, and other types of hazard, will be included in future iterations.
- The detailed plans for each sector were required to address, as a minimum:
    - the identification of critical national infrastructure in each sector
    - current understanding of the risks from river and coastal flooding to critical infrastructure and essential services in each sector;
    - what is already being done directly and indirectly to address deficiencies in resilience to severe disruption from flooding;
    - and further work that will be needed to improve resilience to disruption from flooding to the initial interim standard of resilience to a 0.5 per cent annual probability of flooding." [p. 4]

Description:

- This document sets out a summary of the sector resilience plans described above.
- "The plans set out:
    - The priorities for improving resilience within each sector…
    - Plans to improve resilience…
    - The respective roles and responsibilities of infrastructure operators, lead government departments, devolved administrations and regulators in each sector." [p. 5-6]

2.1.4 Australia

2.1.4.1 Critical Infrastructure Resilience Strategy

Title: Critical Infrastructure Resilience Strategy
Author(s): Australian Government
Organization: Australian Government
Publisher: Australian Government
Publishing Location: Australia
Edition: Unavailable
Pages: 40
Retrieved from: Trusted Information Sharing Network (TISN) website
Hyperlink:
http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf
Date of Publication: 2010

Aim:

- "The aim of this Strategy is the continued operation of critical infrastructure in the face of all hazards, as this critical infrastructure supports Australia's national defence and national security, and underpins our economic prosperity and social wellbeing. More resilient critical infrastructure will also help to achieve the continued provision of essential services to the community." [p. 8]

Objectives:

1. "Critical infrastructure owners and operators (including the Australian Government) are effective in managing foreseeable risks to the continuity of their operations, through an intelligence and information led, risk informed approach." [p. 12]
2. "Critical infrastructure owners and operators enhance their capacity to manage unforeseen or unexpected risk to the continuity of their operations, through an organisational resilience approach." [p. 13]

Description:

- "This Strategy describes the Australian Government's approach to enhancing the resilience of our critical infrastructure to all hazards…
- This Strategy encourages and enables critical infrastructure organisations, through a range of initiatives and activities, to better manage both foreseeable and unforeseen or unexpected risks to their critical infrastructure assets, supply chains and networks." [p. 4]
- This Strategy includes descriptions of six strategic imperatives which must be implemented in order to achieve the Australian government's aims and objectives for building critical infrastructure resilience.

2.1.4.2 Critical Infrastructure Resilience Strategy Supplement: An Overview of Activities to Deliver the Strategy

Title: Critical Infrastructure Resilience Strategy Supplement: An Overview of Activities to Deliver the Strategy
Author(s): Australian Government
Organization: Australian Government
Publisher: Australian Government
Publishing Location: Australia
Edition: Unavailable
Pages: 24
Retrieved from: Trusted Information Sharing Network (TISN) website
Hyperlink:
http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy+Supplement.pdf
Date of Publication: 2010

Description:

- This document is a supplement to the Australian Government's *Critical Infrastructure Resilience Strategy* (2010).
- The *Strategy* identified six strategic imperatives which are necessary to realize the Australian Government's aims and objectives for critical infrastructure resilience.
- This companion document outlines the activities that are associated with the delivery of the strategic imperatives. Recognizing the interconnectedness of the strategic imperatives, the document also explains how each imperative supports and feeds into the others.

2.1.4.3 Critical Infrastructure Protection National Strategy

Title: Critical Infrastructure Protection National Strategy
Author(s): Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection
Organization: Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection
Publisher: Unavailable
Publishing Location: Australia
Edition: Version 2.1
Pages: 12
Retrieved from: N/A
Hyperlink: http://www.ict-industry-reports.com/wp-content/uploads/2009/11/2004-australian-critical-infrastructure-protection-national-strategy-march-2004.pdf
Date of Publication: March 12, 2004

Purpose:

- "This strategy is intended to provide an overarching statement of principles for critical infrastructure protection in Australia, and outline the major tasks and assign responsibilities necessary for their application…
- The strategy provides guidance for the medium term, with a three to five year outlook. It will require detailed implementation plans by governments and industry sectors, and will require the development of interfaces with many other areas of public policy." [p. 1]

Audience:

- "This strategy is for use not only by government, but also by the owners and operators of infrastructure, their representative bodies, professional associations, regulators and standards setting institutions." [p. 1]

Additional Information:
This strategy outlines and describes key concepts and activities for improving critical infrastructure. They are:

- Definition
- All Hazards
- Scope of Critical Infrastructure
- Identification of Critical Infrastructure
- Principles of Critical Infrastructure Protection
- Achieving a Business-Government Partnership
- Coordination within and Between Australian Governments
- Information Sharing
- Response to Predominant Risks and Threats
- Relationship with the National Counter Terrorism Arrangements
- Responsibilities
- Research
- Public Information
- Measurable Objectives
- The Role of Regulation
- Implementation

2.1.4.4 The Development of Australia's Federal Critical Infrastructure Policy, 1978-2010

Title: The Development of Australia's Federal Critical Infrastructure Policy, 1978-2010
Author(s): Ms. Kate O'Donnell
Organization: N/A
Publisher: ARC Centre of Excellence in Policing and Security (CEPS)
Publishing Location: Australia
Edition: Unavailable
Pages: 6
Retrieved from: ARC Centre of Excellence in Policing and Security (CEPS) Briefing Paper, Issue 10
Hyperlink:
http://www.ceps.edu.au/CMS/Uploads/file/K%20ODonnell%20The%20Development%20of%20Australias%20Federal%20Critical%20Infrastructure.pdf
Date of Publication: January 2010

Overview:
"Australia's strategy for managing national security is set out in a number of complex and interrelated policy documents that span multiple agencies. The strategy for protecting what is now known as "critical infrastructure" and "designated critical infrastructure" is only one part of this complex policy fabric that has developed over time. This paper summarises key parts of the federal critical infrastructure (CI) protection policy trajectory in the period 1978 – 2010." [p. 1]

2.1.5 Germany

2.1.5.1 National Strategy for Critical Infrastructure Protection (CIP Strategy)

Title: National Strategy for Critical Infrastructure Protection (CIP Strategy)
Author(s): Federal Republic of Germany, Federal Ministry of the Interior
Organization: Federal Republic of Germany, Federal Ministry of the Interior
Publisher: Federal Ministry of the Interior
Publishing Location: Berlin
Edition: Unavailable
Pages: 18
Retrieved from: Federal Ministry of the Interior website
Hyperlink:
http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf
Date of Publication: June 17, 2009

Description:

- "The National Strategy for Critical Infrastructure Protection summarizes the Federal Administration's aims and objectives and its political-strategic approach that is already applied in practice and, for the field of information technology, is included, for example, also in the National Plan for Information Infrastructure Protection (Nationaler Plan zum Schutz der Informationsstrukturen - NPSI); the Strategy also is the starting point for consolidating the results achieved so far and for further developing them in view of novel challenges." [p. 3]

Additional Information:
This document covers the following subject areas:

- Guiding Policy Concept
- Progress made so far, and present status
- Criticality of infrastructure, and areas of responsibility
- Threats, risks, vulnerabilities and risk culture
- Strategic aims
- Co-operation, voluntary self-regulation, and legal regulations
- Implementation procedure
- International co-operation

2.1.5.2 National Plan for Information Infrastructure Protection

Title: National Plan for Information Infrastructure Protection
Author(s): Federal Ministry of the Interior
Organization: Federal Ministry of the Interior
Publisher: Bundesministerium des Innern
Publishing Location: Berlin
Edition: Unavailable
Pages: 23
Retrieved from: Unavailable
Hyperlink:
http://msmunir.batan.go.id/iaea2008/Reference_material/NatlStd/GER_National_Plan_for_Information_Infrastructure_Protection.pdf
Date of Publication: October 2005

Background:

- "Today our internal security is...inseparable from secure information infrastructures; their protection is a key priority for our national security policy. For this reason, the present National Plan has been drawn up under the aegis of the Federal Ministry of the Interior. Implementing this plan will help strengthen the defence of Germany's information infrastructures against global threats." [p. 2]

Description:

- The National Plan for Information Infrastructure Protection sets out three strategic objectives. They are:
  - "Prevention: Protecting information infrastructures adequately
  - Preparedness: Responding effectively to IT security incidents
  - Sustainability: Enhancing German competence in IT security/Setting international standards" [p. 5]
- The plan outlines goals that the Federal government should achieve in order realize these objectives.

2.1.6 Multi/International

2.1.6.1 Canada-United States Action Plan for Critical Infrastructure

Title: Canada-United States Action Plan for Critical Infrastructure
Author(s): U.S. Department of Homeland Security, Public Safety Canada
Organization: U.S. Department of Homeland Security, Public Safety Canada
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 9
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf
Date of Publication: 2010

Background:

- This *Action Plan* reflects Canada and the United States' first cross-border initiative to strengthen critical infrastructure resilience.

Objective:

- "The purpose of the Canada-U.S. Action Plan is to strengthen the safety, security and resiliency of Canada and the United States by establishing a comprehensive cross-border approach to critical infrastructure resilience. Pressures to take action and advance an integrated approach to critical infrastructure are mounting." [p. 3]

Description:

- "The Canada-U.S. Action Plan is based on three objectives that will allow Canada and the United States to strengthen our collective readiness for critical infrastructure disruptions." [p. 5]
  They are:
  - "Building partnerships,
  - Improved information sharing, and
  - Risk management" [p. 5]
- This *Action Plan* describes key components of these objectives, and outlines action items that are needed to achieve them.
- Lastly, this document concludes with an overview of the initiatives that will be undertaken in order to implement the *Action Plan*.

2.1.6.2 CRN Report - Factsheet - Lessons from the US National Infrastructure Protection Plan (NIPP) for Sector-Specific and Cross-sector Risk Analysis in Switzerland

Title: CRN Report - Factsheet - Lessons from the US National Infrastructure Protection Plan (NIPP) for Sector-Specific and Cross-sector Risk Analysis in Switzerland
Author(s): Elgin Brunner, Myriam Dunn Cavelty
Organization: Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich
Publisher: Centre for Security Studies (CSS), ETH Zürich
Publishing Location: Zürich, Switzerland
Edition: N/A
Pages: 17
Retrieved from: Centre for Security Studies (Switzerland) website
Hyperlink: http://www.css.ethz.ch/publications/DetailansichtPubDB?rec_id=2077
Date of Publication: July 2011

Description:

- "This fact sheet analyses the United States (US) National Infrastructure Protection Plan (NIPP), which sets forth a comprehensive risk management framework and clearly defines roles and responsibilities.
- It will particularly examine the updated version of the NIPP (NIPP 2009), which takes an all-hazards approach and emphasizes the integration of the resilience concept as well as the use of a common risk assessment approach, including the core criteria for these analyses to allow the comparison of risk across sectors.
- The aim is to identify lessons learned for Switzerland's sector-specific and cross-sector risk analysis in Critical Infrastructure Protection (CIP)." [p. 4]

Additional Information:
"The factsheet has three main parts:

- The first part provides a short overview of how the United States organizes CIP and of the role that the NIPP plays.
- The second looks more closely at the integrated risk analysis and management framework of the NIPP.
- The third and final part identifies implications for Switzerland's own methodological guideline for risk analysis in CIP that is currently being developed by the Swiss Federal Office for Civil Protection (FOCP)." [p. 4]

2.1.6.3 Protecting Critical Infrastructure in the EU

Title: Protecting Critical Infrastructure in the EU
Author(s): Centre for European Policy Studies (CEPS)
Organization: Centre for European Policy Studies (CEPS)
Publisher: Centre for European Policy Studies (CEPS)
Publishing Location: Brussels
Edition: Unavailable
Pages: 106
Retrieved from: Centre for European Policy Studies (CEPS) Task Force Report
Hyperlink: http://www.ceps.eu/mwg-internal/de5fs23hu73ds/progress?id=RVhbflZai6
Date of Publication: 2010

Description:

- This report presents the outputs of the discussions held within the Centre for European Policy Studies (CEPS) Task Force on Critical Infrastructure Protection.
- It contains the opinions of the participants regarding European policy on critical infrastructure and its future directions.

Additional Information:
This report covers the following areas:

- Main Policy Recommendations
- Executive Summary
- Introduction: A paradigm shift?
- Critical infrastructure: Basic facts and existing policies
- Identifying the policy challenge
- Addressing policy challenges: Towards a holistic approach to C(I)IP

2.1.6.4 International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies

Title: International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies
Author(s): Elgin M. Brunner and Manuel Suter
Organization: Centre for Security Studies, ETH (Swiss Federal Institute of Technology) Zürich
Publisher: Centre for Security Studies, ETH (Swiss Federal Institute of Technology) Zürich
Publishing Location: Zürich, Switzerland
Edition: 4th ed.
Pages: 652
Retrieved from: ETH Institutional repository, E-collection
Hyperlink: http://e-collection.library.ethz.ch/eserv/eth:31095/eth-31095-01.pdf
Date of Publication: 2008-2009

Purpose:

- "The CIIP [Critical Information Infrastructure Protection] Handbook focuses on national governmental efforts to protect critical (information) infrastructure. The overall purpose of the International CIIP Handbook is to provide an overview of CII protection practices in an increasingly broad range of countries." [p. 39]

Audience and Scope:

- "The Handbook is aimed mainly at security policy analysts, researchers, and practitioners.
- It can be used either as a reference work for a quick overview of the state of the art in CIIP policy formulation, or as a starting point for further, more in-depth research. As in previous years, the Handbook does not offer any benchmarking or analysis of these policies. This is done in additional publications of the Center for Security Studies." [p. 39]

Description:

- This report provides an overview of critical infrastructure protection practices in 25 countries. For each country, the following points are discussed:
    - "Definition of critical sectors...
    - Past and present CIIP initiatives and policy...
    - Organizational structures...
    - Early-warning approaches and public outreach...
    - Laws and legislation" [p. 39-40]

2.1.6.5 CRN Report - Focal Report 3 - Critical Infrastructure Protection: Cybersecurity - Recent Strategies and Policies: An Analysis

Title: CRN Report - Focal Report 3 - Critical Infrastructure Protection: Cybersecurity - Recent Strategies and Policies: An Analysis
Authors and Contributors: Elgin Brunner, Anna Michalkova, Manuel Suter, Myriam Dunn Cavelty
Organization: Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH (Swiss Federal Institute of Technology) Zürich
Publisher: Center for Security Studies (CSS), ETH Zürich
Publishing Location: Zürich, Switzerland
Edition: N/A
Pages: 22
Retrieved from: Centre for Security Studies (Switzerland) website
Hyperlink: http://www.css.ethz.ch/publications/pdfs/Focal-Report-3-CIP.pdf
Date of Publication: August 2009

Background:

- "This focal report concentrates on cybersecurity. First, cybersecurity is regarded as a key element of CIP since the mid 1990s. Second, in both previous reports, the growing and continued attention on the cyberspace dimension of CIP was identified as a trend. Third, many countries have recently launched new cybersecurity strategies or noteworthy policy papers on this topic." [p. 4]

Description:

- "The report at hand has four parts:
  1. The first part focuses on a) cybersecurity definitions and b) threat perceptions – i.e., which threats the strategies identify and what is threatened according to these documents.
  2. The second part looks at the proposed responses.
  In general, the strategies focus on four measures: public-private collaboration for incident response and prevention; public awareness-raising; institutional responses (creation of agencies responsible for cybersecurity); and international cooperation.
  3. In the third part, this report discusses the findings with a special focus on the implications for Switzerland.
  4. Finally, an annotated bibliography gives an overview of the major recent and relevant documents and articles on cybersecurity." [p. 5]

2.1.6.6 CRN Report, Focal Report 1 - Critical Infrastructure Protection

Title: CRN Report, Focal Report 1 - Critical Infrastructure Protection
Author(s): Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH (Swiss Federal Institute of Technology) Zürich
Organization: Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH (Swiss Federal Institute of Technology) Zürich
Publisher: Center for Security Studies (CSS), ETH Zürich
Publishing Location: Zürich, Switzerland
Edition: N/A
Pages: 30
Retrieved from: Centre for Security Studies (Switzerland) website
Hyperlink: http://www.css.ethz.ch/publications/pdfs/Focal-Report-1-CIP.pdf
Date of Publication: October 2008

Background:

- This is the first of two annual "focal reports" (Fokusberichte) compiled by the Centre for Security Studies (CSS) at ETH Zurich.
- These reports discuss critical infrastructure protection and risk analysis, with the aim of stimulating discussion and providing information about new trends and insights.

Description:
This report has two sections. They are:

1. Critical Infrastructure Protection Policies:
   "First, it identifies three trends in CIP based on the review of governmental protection policies and the science monitoring. This is followed by an extensive annotated bibliography, which covers texts and resources for critical infrastructure protection in three sections: policy documents, academic texts, and internet resources." [p. 1]

2. Security Threats to the Energy Infrastructure
   "Second, this report focuses on a topic that has gained increased attention in the last couple of years: attacks on the energy infrastructure. This topic is still largely under-researched and is usually not discussed under the larger heading of CIP, despite its link to the issue. It is particularly interesting because it deals with physical attacks rather than cyber-attacks, which still dominate the general CIP literature. The second section is also followed by an annotated bibliography that provides some recently produced resources on threats to the energy infrastructure." [p. 1]

2.1.6.7 Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security

Title: Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security
Author(s): Kathryn Gordon (Senior Economist, OECD) and Maeve Dion (George Mason University Law School)
Organization: Organization for Economic Co-operation and Development (OECD)
Publisher: Organization for Economic Co-operation and Development (OECD)
Publishing Location: Unavailable
Edition: Unavailable
Pages: 11
Retrieved from: Organization for Economic Co-operation and Development (OECD) website
Hyperlink: http://www.oecd.org/dataoecd/2/41/40700392.pdf
Date of Publication: May 2008

Description:

- "Drawing on notifications made under OECD investment instruments and on other publicly available information, this note presents a factual survey of governments' general strategies for protecting critical infrastructure and of the role that investment policy plays in these strategies." [p. 3]

Additional Information:
"This note contains the following sections:

- Section II. Definitions of Critical Infrastructure
- Section III. General policy frameworks for the protection of critical infrastructure
- Section IV. Review of foreign investment policies in infrastructure sectors
- Section V. The contribution of investment policy to critical infrastructure protection" [p. 3]

2.2 Frameworks and Guidelines Related to CI

2.2.1 Canada

2.2.1.1 Risk Management Guide for Critical Infrastructure Sectors

Title: Risk Management Guide for Critical Infrastructure Sectors
Author(s): Public Safety Canada
Organization: Public Safety Canada
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Version 1.0 (Initial Version)
Pages: 37
Retrieved from: Public Safety website
Hyperlink: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/rmgcis-ggrsie-eng.pdf
Date of Publication: July 2010

Purpose:

- "Recognizing that the impacts of disruptions can cascade across sectors and jurisdictions, the purpose of this document is to provide practical guidance for implementing a coordinated, all-hazards approach to critical infrastructure risk management." [p. 2]

Additional Information:

- This guide is adapted from the ISO 31000 International Standard: "Risk Management – Principles and guidelines on implementation", and includes the following sections:
  1. Overview, Principles and Process
  2. Sector Networks: Communication and consultation
  3. Sector Overviews: Part 1 – Sector Operations
  4. Sector Overviews: Part 2 – Sector Risk Profile
  5. Sector Overviews: Part 3 – Sector Workplan
  6. Ongoing improvement and feedback

- Sections 2 through 6 focus on implementation and contain the following subsections:
  - *Key Elements*: The inputs and expected deliverables.
  - *Implementation*: Recommended approaches to implementation.
  - *Considerations*: Questions, issues and challenges to consider." [p. 2]

2.2.2 United States

2.2.2.1 Regional Disaster Resilience: A Guide for Developing an Action Plan

Title: Regional Disaster Resilience: A Guide for Developing an Action Plan
Author(s): The Infrastructure Security Partnership (TISP)
Organization: The Infrastructure Security Partnership
Publisher: Unavailable
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 68
Retrieved from: The Infrastructure Security Partnership website
Hyperlink: http://www.tisp.org/tisp/file/Template_TISP%20Layout_v29(2).pdf
Date of Publication: September 2011

Purpose, Scope and Audience:

- "The RDR Guide is intended to provide practitioners and experts from government, the private sector and other interested organizations with a tested holistic approach, framework, and guidance to develop and implement a flexible and dynamic Action Plan to improve the resilience of their organization, community or region for all-hazards incidents and disasters." [p. 7]

Description:

- The RDR Guide is a "roadmap that describes a step-by-step process that can be customized to develop a cross-sector, multi-jurisdiction strategy to improve capabilities to deal with any major incident or disaster." [p. 1]

Additional Information:
"The RDR Guide includes basic information -

- "Key definitions and fundamental principles underlying the need for, and how to achieve regional resilience;
- Background on infrastructure interdependencies and potential impacts;
- A comprehensive list of focus areas and priority issues that should be considered; and
- A checklist of typical preparedness gaps with recommended activities to address them." [p. 1]

"More importantly, the Guide

- Outlines a multi-step approach to develop a regional resilience Action Plan through identifying and bringing together in partnership the necessary broad stakeholder base of public, private and non-profit organizations;
- Conducting workshops, a baseline assessment of capabilities and needs;
- An interdependencies exercise; and
- Other activities to develop a stakeholder-validated resilience roadmap." [p. 1]

"Lastly, the Guide

- "Addresses the challenges facing Action Plan implementation and offers practical ways to organize, maintain, and sustain continued stakeholder collaboration and interest and obtain necessary funding and expertise to move towards regional resilience." [p. 1]

- "The RDR guide lists 14 focus areas and respective detailed priority issues covering all hazards, and recommends short, medium and longer-term activities to address the respective shortfalls." [p. 5]

2.2.2.2 Critical Infrastructure & Key Resources - Using Commercialization to Develop Solutions Efficiently and Effectively

Title: Critical Infrastructure & Key Resources - Using Commercialization to Develop Solutions Efficiently and Effectively
Author(s): U.S. Department of Homeland Security
Editors: Office of Infrastructure Protection, National Protection and Programs Director, U.S. Department of Homeland Security; and Thomas A. Cellucci, Ph.D., MBA, Chief Commercialization Officer, U.S. Department of Homeland Security
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: Unavailable
Edition: Unavailable
Pages: 423
Retrieved from: U.S. Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/st_cikr_requirements_book_jan_2010.pdf
Date of Publication: January 2010

Purpose:

- "Among the challenges facing DHS is how to gather and refine the needs and requirements of its various stakeholders, who represent a wide variety of mission spaces and operating environments, in a cost-effective and efficient manner.
- The purpose of this guide is simple and straightforward: to enable the reader to effectively engage with the Department of Homeland Security in a simple and straightforward way.
- This resource will facilitate methods to articulate detailed operational requirements and define mission problems effectively, specifically those of the CIKR community.
- Readers will be able to better understand stakeholder interaction channels through various organizational elements and learn how to improve the communication of their needs and requirements to others in DHS, other Federal agencies, or the private sector." [p. 5]

Additional Information:
This book provides:

a) "introduction to working with DHS and its organizational elements responsible for assisting CIKR owners and operators and
b) an easy-to-follow template that will enable the generation and articulation of detailed operational requirements." [p. 6]

2.2.2.3 National Incident Management System

Title: National Incident Management System
Author(s): U.S. Department of Homeland Security
Organization: U.S. Department of Homeland Security
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 170
Retrieved from: Federal Emergency Management Agency (FEMA) website
Hyperlink: http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf
Date of Publication: December 2008

Description:

- "The *National Incident Management System* (NIMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment." [p. 1]
- "NIMS is not an operational incident management or resource allocation plan. NIMS represents a core set of doctrines, concepts, principles, terminology, and organizational processes that enables effective, efficient, and collaborative incident management." [p. 3]

Additional Information:
The NIMS components are:

- Preparedness
- Communications and Information Management
- Resource Management
- Command and Management
- Ongoing Management and Maintenance

2.2.2.4 A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level

Title: A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level
Author(s): U.S. Department of Homeland Security
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: Unavailable
Edition: Unavailable
Pages: 100
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf
Date of Publication: September 2008

Audience:

- "Homeland Security Advisors (HSAs), State Administrative Agencies (SAAs), Urban Area Working Groups (UAWGs), regional groups and coalitions, and other State and local agency leads with responsibilities that include aspects of homeland security...In addition, much of the information presented will be useful to those responsible for homeland security practices and initiatives at the territorial, tribal, or local level." [p. 1-2]

Description:

- This document provides an interpretation of the requirements of the National Infrastructure Protection Plan (NIPP) for its application to non-Federal levels (state, regional, local, tribal and territorial).
- The guide supports government entities as they establish their functions in CIKR protection. It does so by describing the attributes, capabilities, needs, and processes which must be included in non-Federal CIKR plans in order to ensure their alignment with the NIPP.

Additional Information:

- The elements required for non-Federal CIKR protection plans and resiliency strategies are:
    - "CIKR protection roles and responsibilities;
    - Building partnerships and information sharing;
    - Implementing the NIPP Risk Analysis/Management Framework;
    - Developing Procedures for data use and protection;
    - Leveraging ongoing sector-based activities for CIKR protection and resiliency; and
    - Integrating Federal and sector CIKR protection activities.
- This document speaks to all of these points, describing their importance and purpose. It is intended to serve as a "why-to" rather than a "how-to" guide." [p. 1]

2.2.2.5 Critical Infrastructure and Key Resources Support Annex

Title: Critical Infrastructure and Key Resources Support Annex
Author(s): Unavailable
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 36
Retrieved from: Federal Emergency Management Agency (FEMA) website
Hyperlink: http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf
Date of Publication: January 2008

Purpose and Description:

- "This annex describes policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting, and restoring critical infrastructure and key resources (CIKR) of the United States and its territories and possessions during actual or potential domestic incidents. The annex details processes to ensure coordination and integration of CIKR-related activities among a wide array of public and private incident managers and CIKR security partners within immediate incident areas as well as at the regional and national levels. Specifically, this annex does the following:
    - Describes roles and responsibilities for CIKR preparedness, protection, response, recovery, restoration, and continuity of operations relative to National Response Framework (NRF) coordinating structures and National Incident Management System (NIMS) guiding principles.
    - Establishes a concept of operations for incident-related CIKR preparedness, protection, response, recovery, and restoration.
    - Outlines incident-related actions (including preresponse and postresponse) to expedite information sharing and analysis of actual or potential impacts to CIKR and facilitate requests for assistance and information from public- and private-sector partners." [p. 1]

Scope and Audience:

- "Processes outlined herein apply to Federal departments and agencies during incidents with potential or actual CIKR impacts—and may apply to, or involve, incident managers and security partners at other levels of government and the private sector, including CIKR owners and operators." [p. 2]

2.2.2.6 National Preparedness Guidelines

Title: National Preparedness Guidelines
Author(s): U.S. Department of Homeland Security
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: Unavailable
Edition: Unavailable
Pages: 51
Retrieved from: Department of Homeland Security's Lessons Learned Information Sharing website,
Hyperlink: https://www.llis.dhs.gov/docdetails/details.do?contentID=26718
Date of Publication: September 2007

Abstract:
"As part of the effort to develop a national domestic all-hazards preparedness goal, the Department of Homeland Security released the Interim National Preparedness Goal in March 2005. Publication of the National Preparedness Guidelines (Guidelines) finalizes development of the national goal and its related preparedness tools. The Guidelines, including the supporting Target Capabilities List, simultaneously published online, supersedes the Interim National Preparedness Goal and defines what it means for the Nation to be prepared for all hazards. The Guidelines reinforce the fact that preparedness is a shared responsibility. They were developed through an extensive process that involved more than 1,500 Federal, State, and local officials and more than 120 national associations. They also integrate lessons learned following Hurricane Katrina and a 2006 review of States' and major cities' emergency operations and evacuation plans"[5].

Purpose:
"The purposes of the *Guidelines* are to:

- Organize and synchronize national (including Federal, State, local, tribal, and territorial) efforts to strengthen national preparedness;
- Guide national investments in national preparedness;
- Incorporate lessons learned from past disasters into national preparedness priorities;
- Facilitate a capability-based and risk-based investment planning process; and
- Establish readiness metrics to measure progress and a system for assessing the Nation's overall preparedness capability to respond to major events, especially those involving acts of terrorism." [p. 1]

Description:

- "The *Guidelines* include a vision, capabilities, and priorities for national preparedness." [p. 1]

[5]From https://www.llis.dhs.gov/docdetails/details.do?contentID=26718

2.2.2.7 Target Capabilities List

Title: Target Capabilities List
Author(s): U.S. Department of Homeland Security
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: Unavailable
Edition: Unavailable
Pages: 588
Retrieved from: FEMA website
Hyperlink: http://www.fema.gov/pdf/government/training/tcl.pdf
Date of Publication: September 2007

Background:

- The *Target Capabilities List* (TCL) is a companion to the *National Preparedness Guidelines*. Together, these two documents establish an all-hazards framework for a "fully integrated, adaptable, all-hazards national preparedness system." [p. v]

Scope:

- "The TCL should be viewed as a reference document or guide to preparedness. It should not serve as a prescription for program requirements or resource commitments." [p. 12]

Description:

- "The TCL is a national-level, generic model of operationally ready capabilities defining all-hazards preparedness. Users should refer to the TCL to assess capabilities, identify needs, and inform plans and strategies taking into account their risk…
- The TCL supports an all-hazards approach to building interchangeable, flexible capabilities needed to address a broad range of incidents to include: terrorist attacks, natural disasters, health emergencies, and other major incidents.
- It currently identifies 37 capabilities that were developed with the active participation of stakeholders representing all levels of government, non-governmental organizations, and the private sector." [p. 1]

Additional Information:

- "Each capability includes a definition; outcome; preparedness and performance activities, tasks, and measures.
- The TCL also identifies the role of governmental and non-governmental organizations, the private sector, and citizens in building and maintaining capabilities." [p. 1]

2.2.3 United Kingdom

2.2.3.1 Keeping the Country Running: Natural Hazards and Infrastructure

Title: Keeping the Country Running: Natural Hazards and Infrastructure
Author(s): Cabinet Office UK, in partnership with representatives from organizations under the Critical Infrastructure Resilience Programme
Organization: Cabinet Office
Publisher: Cabinet Office
Publishing Location: London, UK
Edition: N/A
Pages: 98
Retrieved from: Cabinet Office website (UK)
Hyperlink: http://www.cabinetoffice.gov.uk/sites/default/files/resources/natural-hazards-infrastructure.pdf
Date of Publication: October 2011

Purpose:

- This guide encourages "infrastructure owners and operators, emergency responders, industry groups, regulators, and government departments to work together to improve the resilience of critical infrastructure and essential services…
- The Guide shares best practice and advice to enable organisations to continuously improve their infrastructure's resilience to natural hazards. It supplements existing guidance and fills gaps identified during the consultation on the Strategic Framework and Policy Statement (March 2010)." [p. 7]

Scope:

- This Guide focuses on improving resilience to natural hazards. However, it does not discuss the causes of infrastructure vulnerability to natural hazards.
- In addition, it does not provide an assessment of the UK's infrastructure resilience.

Description:

- "Divided into four sections, the Guide sets out the principles underpinning infrastructure resilience and provides advice and practical guidance on risk assessment for natural hazards, standards of resilience, corporate governance, information sharing and the role for economic regulators." [p. 5]

2.2.3.2 Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards

Title: Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards
Author(s): Cabinet Office
Organization: Cabinet Office
Publisher: Cabinet Office
Publishing Location: London, UK
Edition: Unavailable
Pages: 26
Retrieved from: UK government national archives
Hyperlink:
http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/349103/strategic-framework.pdf
Date of Publication: March 2010

Purpose:

- "This Strategic Framework and Policy Statement establishes a cross-sector programme to improve the resilience of critical infrastructure and essential services to disruption from natural hazards. The purpose is to develop a shared, consistent, proportionate and risk-based approach to delivering reductions in vulnerability over a number of years, as envisaged by Sir Michael Pitt in his reports on the floods of summer 2007.
- As Sir Michael recommended, the Framework is intended to encompass a co-ordinated approach to driving up the resilience of critical infrastructure. The main goal is to identify and assess risks from natural hazards, and thereafter to develop a range of options to avoid, transfer, accept, reduce or share those risks. Options could vary from the provision of physical protection through the relocation of assets, or the provision of alternative supplies, or improved arrangements for emergency response." [p. 5]

Audience:

- "This Framework is primarily directed at central government departments, regulators, relevant public sector bodies and critical infrastructure owners." [p. 5]

Description:

- This document "describes the policy intent, scope, aims, work streams and timescales of the Critical Infrastructure Resilience Programme." [p. 5]

Additional Information:
The Framework covers the following areas:

- The Critical Infrastructure Resilience Programme
  (Definitions, Aims, Principles, Scope, Work Streams, Timetable)
- Policy and Standards
  (The Impact of natural hazards, Flood resilience standards)
- Roles and responsibilities
  (Cabinet office, Government departments, Devolved administrations, Regulators, Infrastructure owners and operators, Centre for the protection of national infrastructure, Environment agency)

2.2.3.3 Interim Guidance to the Economic Regulated Sectors - Water, Energy, Transport and Communication

Title: Interim Guidance to the Economic Regulated Sectors - Water, Energy, Transport and Communication
Author(s): Cabinet Office
Organization: Cabinet Office
Publisher: Cabinet Office
Publishing Location: London, UK
Edition: N/A
Pages: 24
Retrieved from: Cabinet Office website
Hyperlink: http://www.cabinetoffice.gov.uk/sites/default/files/resources/interim-guidance-ers.pdf
Date of Publication: March 2010

Aim:

- "This guidance builds upon the general guidance set out within the *Strategic Framework and Policy Statement* (SFPS)…
- This document provides detailed interim guidance to the economic regulated sectors, not solely the regulators." [p. 4-5]

Scope:

- "Resilience work undertaken in the four regulated utility sectors: water, energy, communications and transport." [p. 5]

Description:

- "This guidance is in the form of eight considerations. The use of the term "considerations" is intentional given that there is no blanket set of regulatory powers or duties across the regulated sectors: some of the considerations are related to regulators while some belong squarely with industry. Taken together these considerations provide a basis for a joint approach to resilience building." [p. 4-5]

Additional Information:
The Eight considerations are:

1. "Reporting on resilience
2. Vulnerable site monitoring schemes
3. Business Continuity Management (BS25999)
4. Inconsistent standards
5. Formalising innovative funding initiatives
6. Improving resilience business cases
7. Exemption clauses in service standards
8. Data impact on financing redundancy" [p. 6-7]

2.2.3.4 Secure and Resilient: A Strategic Framework for Critical National Infrastructure in Scotland

Title: Secure and Resilient: A Strategic Framework for Critical National Infrastructure in Scotland
Author(s): The Scottish Government
Organization: The Scottish Government
Publisher: Scottish Government
Publishing Location: Edinburgh
Edition: Unavailable
Pages: 34
Retrieved from: Emergency Planning college website
Hyperlink:
http://www.epcollege.com/EPC/media/MediaLibrary/Knowledge%20Hub%20Documents/A%20Strategic%20Framework/Secure-Resilient.pdf?ext=.pdf
Date of Publication: March 2011

Purpose:

- "The purpose of this document is to provide clear guidance and a strategic framework within which Scottish Government and key public and private sector Stakeholders in Scotland, can contribute positively within the devolution framework to the overall UK Government arrangements for infrastructure protection and resilience, specifically on CNI [Critical National Infrastructure]…
- This strategy sits under and meshes with the UK National Security Strategy, the UK CONTEST Strategy and the UK CNI Protection Framework. It is intended to describe in more detail the Scottish Government contribution to these UK strategies including aims, responsibilities and delivery arrangements.
- It also clarifies areas where Scottish Government leads (on devolved matters) and areas which are reserved where Scottish Government aims to work closely in support of Whitehall departments." [p. 7]

Scope:

- "This strategy focuses on Scotland's contribution to infrastructure security and resilience with a specific focus on CNI assets.
- In the short term, the focus of the strategy is to enhance the security and resilience of the Critical National Infrastructure assets in Scotland. In the medium term to longer term, the strategy will extend to other infrastructure which may be of local or Scottish significance but not critical on the UK scale." [p. 7]
- This framework takes an 'all risks' approach to CNI security and resilience.

Additional Information:
This Strategy offers guidance in the following areas:

- Strategic Context
- Defining Critical National Infrastructure
- Threat and Risk Ownership
- Strategy for CNI in Scotland
- Delivering the Strategy

2.2.4 Australia

2.2.4.1 National Guidelines for Protecting Critical Infrastructure from Terrorism

Title: National Guidelines for Protecting Critical Infrastructure from Terrorism
Author(s): National Counter-Terrorism Committee
Organization: National Counter-Terrorism Committee
Publisher: Unavailable
Publishing Location: Australia
Edition: Unavailable
Pages: 24
Retrieved from: Australian National Security website
Hyperlink:
http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(689F2CCBD6DC263C912FB74B15BE8285)~Protecting+Critical+Infrastructure+from+Terrorism+PDF.pdf/$file/Protecting+Critical+Infrastructure+from+Terrorism+PDF.pdf
Date of Publication: 2011

Purpose:

- "The National Guidelines for the Protection of Critical Infrastructure (CI) from Terrorism (the Guidelines) provide a framework for a national, consistent approach on the protection of CI from terrorism for the Commonwealth, State and Territory governments and business.
- They are designed to aid owners/operators of CI in their discussions with jurisdictions (including the Commonwealth Government) about protecting CI from terrorism." [p. 2]

Additional Information:
This document provides guidance on the following areas:

- Introduction
  - Definition of critical infrastructure
  - Critical infrastructure sectors
- Identification of Critical Infrastructure
- An Intelligence-Led, Risk Informed Approach
  - Threat assessments
  - National terrorism public alert system
  - Prevention and preparedness
  - Response and recovery
- Public Information and Media Management

2.2.4.2 Critical Infrastructure Protection in Australia

Title: Critical Infrastructure Protection in Australia
Author(s): National Counter-Terrorism Committee
Organization: Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection
Publisher: Unavailable
Publishing Location: Australia
Edition: Unavailable
Pages: 7
Retrieved from: Emergency Management Australia website
Hyperlink: N/A
Date of Publication: March 25, 2003

Description:

- "Critical infrastructure protection requires a national approach and a cooperative partnership to ensure consistency between the Commonwealth and the States and Territories, and across jurisdictions. To ensure this consistency, this document provides a comprehensive set of principles based on the emergency management 'all hazards, all agencies' approach and are not exclusively focused on the protection of critical infrastructure (either physical or information) from a terrorist attack, but also on security of supply and business continuity." [p. 1]

Additional Information:
The principles set out by this document fall under the following categories:

- Critical Infrastructure (What it is)
- Identification of Critical Infrastructure
- Dependencies and Interdependencies
- Role of the Commonwealth Government
- Role of State and Territory Governments
- National Counter-Terrorism Committee (NCTC)
- Role of State and Territory Police
- Role of Owners and Operators of Critical Infrastructure
- Critical Infrastructure Advisory Council (CIAC)
- Australian Computer Emergency Response Team (AusCERT)
- Roles of other Key Players
- Distribution of Relevant Intelligence and Information
- Risk Management in the Current Environment
- Public Information
- Forward Work Program

2.2.4.3 Western Australia Critical Infrastructure Framework

Title: Western Australia Critical Infrastructure Framework
Author(s): Unavailable
Organization: Government of Western Australia
Publisher: Department of the Premier and Cabinet, Government of Western Australia; and Critical Infrastructure Unit, Western Australia Police
Publishing Location: Western Australia
Edition: Unavailable
Pages: 15
Retrieved from: Government of Western Australia, Office of State Security and Emergency Coordination website
Hyperlink: http://www.ossec.dpc.wa.gov.au/documents/Framework-single.pdf
Date of Publication: April 2007

Description:

- "The Western Australia Critical Infrastructure Protection Framework (the Framework) outlines how Western Australia is meeting its obligations under the national strategy and guidelines and is applying a consistent approach to the protection of infrastructure critical to the State. The Framework is consistent with established arrangements, principles and responsibilities at the State and national level." [p. 4]

Additional Information:
This document establishes a framework by describing Western Australia's approach to critical infrastructure. This framework covers:

- A Co-ordinated Approach to Critical Infrastructure Protection
- What is Critical Infrastructure?
- Critical Infrastructure Protection Program
- Roles and Responsibilities

2.2.4.4 Securing Information in an Outsourcing Environment (Guidance for Critical Infrastructure Providers)

Title: Securing Information in an Outsourcing Environment (Guidance for Critical Infrastructure Providers)
Author(s): Department of Broadband, Communications and the Digital Economy (DBCDE) on behalf of the IT Security Expert Advisory Group (ITSEAG) of the Trusted Information Sharing Network (TISN)
Organization: Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 34
Retrieved from: Trusted Information Sharing Network (TISN)
Hyperlink:
http://www.tisn.gov.au/Documents/Securing%20Information%20in%20an%20Outsourcing%20Environment%20(Guidance%20for%20Critical%20Infrastructure%20Providers).PDF
Date of Publication: June 2011

Purpose:

- "The Guide is intended to provoke dialogue within an organisation's executive to firstly assess whether a service could be suitable for outsourcing, and if so, what are the first principles relating to information security that should be considered." [p. 5]

Description:

- "*Securing Information in an Outsourcing Environment* (*Guidance for Critical Infrastructure Providers*) (The Guide) provides Australian critical infrastructure providers with a resource to assist with the potential information security issues when considering the outsourcing of services or assessing the IT arrangements contained in existing outsourcing contracts." [p. 4]

Additional Information:

- "This guide covers a wide range of potential information security issues that a critical infrastructure provider should consider in an outsourcing environment...The structure of the Guide covers eight (8) information security management elements that occur throughout the outsourcing lifecycle, namely:
  - Information security governance;
  - Roles and Responsibilities;
  - Risk Management and Assessment;
  - Change Management;
  - Assurance and Conformance;
  - Managing information security throughout the outsourcing arrangement;
  - Incident Management; and
  - Termination and Transition." [p. 6]
- "The Guide also briefly discusses cloud computing (the cloud) as a particular outsourcing variant, providing some insights into the differences from traditional outsourcing arrangements and some of the specific information security exposures that should be considered by a critical infrastructure provider." [p. 6]
- The appendices offer several tools and references which may provide further assistance.

2.2.4.5 Secure Your Information - Information Security Principles for Enterprise Architecture

Title: Secure Your Information - Information Security Principles for Enterprise Architecture
Author(s): IT Security Expert Advisory Group of the Trusted Information Sharing Network
Organization: Trusted Information Sharing Network for Critical Infrastructure Protection
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 99
Retrieved from: Department of Broadband, Communications and the Digital Economy (Australian Government) website
Hyperlink: http://www.dbcde.gov.au/__data/assets/pdf_file/0016/70621/SIFT_Full_Report_020707.pdf
Date of Publication: June 2007

Background:

- This document is part of a series of papers released by the Trusted Information Sharing Network (TISN). These papers are intended to assist CEOs and Boards of Directors "understand threats to their IT infrastructure, and to provide recommendations for mitigating those threats." [p. 2]

Description:
This paper responds to the necessity for organizations to "develop an effective governance framework to manage security risks and distribute responsibility." [p. 10] Thus, this document is a resource which provides:

- "Seven key information security principles... for developing an enterprise strategy for information security;
- Approaches for linking these seven key information security principles to your enterprise architecture;
- Recommendations for information security to ensure the integration of security controls throughout the categories of 'people, process and technology'; and
- A self-assessment Checklist for validating an enterprise strategy for information security" [p. 10]

2.2.4.6 Infrastructure Information in the Public Domain: A Guide to Mitigating Security Risks

Title: Infrastructure Information in the Public Domain: A Guide to Mitigating Security Risks
Author(s): Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection
Organization: Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection
Publisher: Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection
Publishing Location: Australia
Edition: Unavailable
Pages: 17
Retrieved from: Trusted Information Sharing Network (TISN) website
Hyperlink: http://www.tisn.gov.au/Documents/Infrastructure_information+in+the+public+domain.pdf
Date of Publication: 2006

Audience:

- "This guide is relevant to businesses that publish or distribute information about infrastructure in the public domain. This can include private organisations, organisations that represent or provide information on behalf of other businesses and government organisations." [p. 2]

Description:

- This Guide addresses the risk that publicly available information can be used to plan an attack. However, this guide is "advisory only and intended to raise awareness of the security implications associated with publishing or distributing potentially sensitive infrastructure information." [p. 3]

Additional Information:

- This guide addresses the following questions:
  - "How do I identify potentially sensitive information?
  - How do I decide whether something needs to be done about the sensitive information?
  - What options are there for lessening the risk?
  - What do I do if someone else is providing information about my business or facility?" [Table of Contents, p. 1]
- In addition, it includes six annexes containing supplementary information.

2.3 Assessments, Reviews, Critiques, and Recommendations for CI Management

2.3.1 Canada

2.3.1.1 DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Programs: Problem Formulation and Solution Strategy

Title: DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Programs: Problem Formulation and Solution Strategy
Author(s): Lynne Genik and Paul Chouinard
Organization: Defence Research and Development Canada (DRDC) – Centre for Security Science (CSS)
Publisher: Defence Research and Development Canada (DRDC) – Centre for Security Science (CSS)
Publishing Location: Canada
Edition: N/A
Pages: 66
Retrieved from: DRDC CSS Technical Memorandum DRDC CSS TM 2012-015
Date of Publication: October 2012

Abstract:
"This paper presents the problem formulation and solution strategy component of the EMBC-DRDC collaborative project agreement for improving EMBC's Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Assurance Programs. The methodology is described; the NATO Code of Best Practice for C2 Assessment and a soft operations research approach were applied, along with aspects of capability based planning, systems engineering, and risk management. Preliminary literature searches were performed and are documented here. Stakeholder groups are described and the questions used to elicit their perspectives on the programs and related issues are presented. The result of the analysis was the identification of program requirements, gaps, and proposed projects by DRDC to address aspects of the gaps. The proposed projects include adapting the Major Events Security Framework for use by EMBC, CI assessment tool development through pilot projects, and contracts for a community resilience framework and scenario mission to task templates, among several others." [p. i]

Note: This paper provides the context for the collaborative project between DRDC and EMBC that is referred to in this document.

2.3.1.2 Solutions to Critical Infrastructure Problems - Essays on Protecting Canada's Infrastructure

Title: z
Editors: Jason Clemens and Brian Lee Crowley
Author(s): Stuart Farson, Douglas Bland, Brigadier-General James Cox, Barry Cooper, Andrew Graham
Organization: Macdonald-Laurier Institute
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 28
Retrieved from: Macdonald-Laurier Institute website, National Security Strategy for Canada Series
Hyperlink: http://www.macdonaldlaurier.ca/files/pdf/Solutions-to-Critical-infrastructure-Problems-February-2012.pdf
Date of Publication: February 2012

Description:

- "This paper contains essays from five scholars...who discuss the vulnerability of Canada's critical infrastructure from their own perspectives, and who offer their thoughts on the means that the federal government might employ to reduce the country's exposure to harm." [p. 4]
- "These five essayists share the view that the federal government needs fundamental changes in its approach to CI security. But the agreement ends there." [p. 6]

2.3.1.3 Canada's Critical Infrastructure: When is Safe Enough Safe Enough?

Title: Canada's Critical Infrastructure: When is Safe Enough Safe Enough?
Author(s): Andrew Graham
Organization: Macdonald-Laurier Institute
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 36
Retrieved from: National Security Strategy for Canada Series, Macdonald-Laurier Institute
Hyperlink: http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf
Date of Publication: December 2011

Purpose:

- "The task here is to describe Canada's CI, identify sources of threat, assess current efforts to address those threats, ask questions that remain to be answered, and suggest themes for moving forward and building on the work that has already been done in government and the private sector." [p. 6]

2.3.1.4 Threats to Canada's Critical Infrastructure

Title: Threats to Canada's Critical Infrastructure
Author(s): Office of Critical Infrastructure Protection and Emergency Preparedness
Organization: N/A
Publisher: Office of Critical Infrastructure Protection and Emergency Preparedness
Publishing Location: Unavailable
Edition: N/A
Pages: 59
Retrieved from: Public Safety website
Hyperlink: http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/ta03-001-eng.pdf
Date of Publication: March 2003

Purpose

- "The purpose of this paper on *Threats to Canada's Critical Infrastructure* is to provide a taxonomy of the natural, accidental and malicious threats that have been identified as those most likely to impact upon Canada's national critical infrastructure. The paper will aim to provide informed forecasting for the relative probability of these threats and hazards." [p. 1]

Audience

- "This report is primarily intended to provide owners and operators of Canadian critical infrastructure (CI) with baseline information regarding potential threats to their networks and systems. Owners and operators are the acknowledged experts with regard to the vulnerabilities they confront, but many have indicated that there is a lack of credible information regarding threats.
- Emergency managers in the public and private sectors could also employ this report to enhance their understanding of the variety of threats and hazards which the Government of Canada is addressing.
- Finally, policy makers at all levels of government may use the paper as a jumping-off point to examine threats and vulnerabilities in CI sectors within their constituencies." [p. 1]

Additional Information:

- This paper begins with an introduction to risk and threat identification and analysis.
- Next, it describes the history, impacts and future trends of natural, accidental and malicious threats in Canada.
- Lastly, this paper includes an annex which describes the key organizations that are responsible for protecting Canadian critical infrastructure.

2.3.1.5 Critical Energy Infrastructure Protection in Canada

Title: Critical Energy Infrastructure Protection in Canada
Author(s): Angela Gendron (Canadian Centre for Intelligence and Security Studies, Carleton University)
Organization: Defence R&D Canada - Centre for Operational Research & Analysis (CORA), Strategic Analysis Section
Publisher: DRDC -CORA
Publishing Location: Ottawa, Canada
Edition: Unavailable
Pages: 60
Retrieved from: Contract Report, DRDC CORA CR 2010-274
Hyperlink: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA535390
Date of Publication: December 2010

Abstract:
"Various government Ministers have affirmed the importance government attaches to the protection of critical energy infrastructure. Nine years after the attacks on 11 September 2001 first focused attention on the potential vulnerability of infrastructure and the economic, social and political consequences of a failure of assurance, a strategy has still not been approved and the assets requiring protection not yet identified. While due respect must be given to the jurisdictional authorities which have been established by the Constitution, international terrorism and newly emerging global threats such as electronic attacks on IT and communication systems have only increased the urgency for Canada to have in place a proactive, seamless system for the protection of those energy assets and services which are so vital to Canada's well-being and prosperity, and North American security. The effectiveness of the draft Strategy and Action Plan proposed by Public Safety Canada will depend upon the voluntary participation of the various public and private sector stakeholders and the extent to which a culture of information sharing and collaboration can be inculcated. Arguably, this is a passive and reactive Plan which gives insufficient attention to deterring and preventing malicious attacks on infrastructure."[p. i]

Description:

- "This study will look at the characteristics of the energy sector with respect to threats, vulnerabilities and risks, before examining how the government of Canada (GOC) has responded to emerging threats; current and proposed government policy with respect to Canada's critical infrastructure; and the governance framework which is in place to implement that policy.

- The study concludes with a brief comment on concerns raised in connection with an 'all-hazards' risk management approach to critical energy infrastructure protection, including the need for a more pro-active strategy." [p. 2]

2.3.1.6 The Ten-Thousand Mile Target: Energy Infrastructure and Terrorism Today

Title: The Ten-Thousand Mile Target: Energy Infrastructure and Terrorism Today
Author(s): Jan K. Fedorowicz
Organization: Canadian Centre of Intelligence and Security Studies (CCISS), the Norman Paterson School of International Affairs
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 23
Retrieved from: Critical Energy Infrastructure Protection, Policy Research Series, No. 2-2007, from the Carleton University website
Hyperlink: http://www3.carleton.ca/cciss/res_docs/ceip/fedorowicz.pdf
Date of Publication: March 2007

Purpose:

- "One way to inform Canadian thinking about this threat is to draw on the experiences of other countries, at least as a starting point for discussion. That is the intent of this paper, which looks at terrorist attacks on critical infrastructure in several countries and considers some of the responses to those attacks. The intention is to see what Canada can learn about what works and what does not in this rapidly evolving area of national security." [p. 1]

Scope:

- "The article will confine itself largely to energy-related infrastructure, which includes the facilities of the oil, gas, nuclear, and hydroelectric industries. It should be added that these particular industries constitute a subset of the expanding discipline of critical infrastructure protection (CIP) that is devoted to ways of protecting vital economic elements from terrorist attacks and other threats. " [p. 1]

Additional Information:
This paper discusses the following, in relation to terrorist attacks:

- The threat
- Historical background
- Defining the danger (Nuclear, Hydroelectric, Petroleum and Natural Gas)
- Forms and effects of attack
- Countermeasures
- Some conclusions

2.3.1.7 Assessment of Terrorist Threats to the Canadian Energy Sector

Title: Assessment of Terrorist Threats to the Canadian Energy Sector
Author(s): Aaron Shull
Organization: Canadian Centre of Intelligence and Security Studies (CCISS), the Norman Patterson School of International Affairs
Publisher: Carleton University
Publishing Location: Ottawa, Canada
Edition: Unavailable
Pages: 20
Retrieved from: Critical Energy Infrastructure Protection Policy Research Series, No. 4, from the Carleton University website
Hyperlink: http://www3.carleton.ca/cciss/res_docs/ceip/shull.pdf
Date of Publication: March 2006

Description:

- "This paper will put forward a critical terrorist threat assessment of Canadian energy systems, with a limited analysis of integrated continental systems.
- The study will examine the types of threats historically posed to the energy infrastructure in Canada and argue that the industry's traditional response capabilities do not match current threats, including the threat of an organized and concerted terrorist attack aimed at strategic elements of the energy system.
- This paper will then examine the Canadian government's recent response to heightened threat levels.
- Next, the study will analyze both the potential of a terrorist attack and the elements of the critical energy infrastructure at greatest risk.
- From here, the paper will briefly outline the direct and indirect consequences of an attack on the Canadian energy infrastructure and set out recommendations to better secure the critical energy infrastructure in Canada." [p. 1]

Additional Information:

- In conclusion, the author argues that "the industry's response capabilities do not match current threats posed by terrorism. The Canadian government's recent response to heightened threat levels has been adequate and has touched on areas ranging from information sharing to emergency preparedness and disaster mitigation strategies." [p. 17]

2.3.1.8 Ports: A Component of Canada's Critical Infrastructure

Title: Ports: A Component of Canada's Critical Infrastructure
Author(s): Michael C. Ircha, PhD, Professor of Civil Engineering, Acting Vice-President (Academic), University of New Brunswick
Organization: University of New Brunswick
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 14-21
Retrieved from: Canadian Ports Magazine, Association of Canadian Port Authorities, Spring 2003
Hyperlink: http://www.unb.ca/transpo/documents/PortsAComponentofCanadasCritInfra..03.pdf
Date of Publication: Spring 2003

Description:

- This paper argues that "ports provide a crucial node in the country's critical transportation infrastructure. Ports need enhanced security to ensure they continue to effectively serve Canadian and diverted US trade." [p. 1-2]

Additional Information:
This paper includes the following sections:

- Port competitiveness and infrastructure development
- Port security in a competitive environment
- Canadian ports as critical infrastructure

2.3.2 United States

2.3.2.1 Critical Infrastructure Protection - DHS Could Better Manage Security Surveys and Vulnerability Assessments

Title: Critical Infrastructure Protection - DHS Could Better Manage Security Surveys and Vulnerability Assessments
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 87
Retrieved from: GAO-12-378, Report to Congressional Requesters, from the Government Accountability Office website
Hyperlink: http://gao.gov/assets/600/591292.pdf
Date of Publication: May 2012

"Why GAO Did This Study:

- Natural disasters, such as Hurricane Katrina, and terrorist attacks, such as the 2005 bombings in London, highlight the importance of protecting CIKR—assets and systems vital to the economy or health of the nation. DHS issued the NIPP in June 2006 (updated in 2009) to provide the approach for integrating the nation's CIKR. Because the private sector owns most of the nation's CIKR—for example, energy production facilities—DHS encourages asset owners and operators to voluntarily participate in surveys or vulnerability assessments of existing security measures at those assets. This includes nationally significant CIKR that DHS designates as high priority.
- In response to a request, this report assesses the extent to which DHS has (1) taken action to conduct surveys and assessments among high–priority CIKR, (2) shared the results of these surveys and assessments with asset owners or operators, and (3) assessed the effectiveness of surveys and assessments and identified actions taken, if any, to improve them. GAO, among other things, reviewed laws, analyzed data identifying high-priority assets and activities performed from fiscal years 2009 through 2011, and interviewed DHS officials.

What GAO Recommends:

- GAO recommends that, among other things, DHS develop plans for its efforts to improve the collection and organization of data and the timeliness of survey and assessment results, and gather and act upon additional information from asset owners and operators about why improvements were or were not made.
- DHS concurred with the recommendations." [Introductory Page]

2.3.2.2 Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities

Title: Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities
Author(s): Stephen L. Caldwell (Director, Homeland Security and Justice Issues)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 29
Retrieved from: GAO-11-537R, Briefing to Congressional Requesters
Hyperlink: http://www.gao.gov/assets/100/97498.pdf
Date of Publication: May 19, 2011

Description:

- "This letter formally discusses a congressional request to review the Department of Homeland Security's framework for securing critical infrastructure and key resources (CIKR), and subsequent agency comments. As such, this correspondence provides information on: (1) how DHS coordinates with CIKR stakeholders to identify overlaps and gaps in CIKR security activities across all sectors, (2) how DHS addresses these potential overlaps in CIKR security activities, and (3) how DHS addresses CIKR security gaps." [p. 1]

2.3.2.3 Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened

Title: Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 46
Retrieved from: GAO-10-772, Report to Congressional Requesters
Hyperlink: http://www.gao.gov/assets/320/310051.pdf
Date of Publication: September 2010

"Why GAO Did This Study:

- According to the Department of Homeland Security (DHS), protecting and ensuring the resiliency (the ability to resist, absorb, recover from, or successfully adapt to adversity or changing conditions) of critical infrastructure and key resources (CIKR) is essential to the nation's security. By law, DHS is to lead and coordinate efforts to protect several thousand CIKR assets deemed vital to the nation's security, public health, and economy. In 2006, DHS created the National Infrastructure Protection Plan (NIPP) to outline the approach for integrating CIKR and increased its emphasis on resiliency in its 2009 update.
- GAO was asked to assess the extent to which DHS (1) has incorporated resiliency into the programs it uses to work with asset owners and operators and (2) is positioned to disseminate information it gathers on resiliency practices to asset owners and operators. GAO reviewed DHS documents, such as the NIPP, and interviewed DHS officials and 15 owners and operators of assets selected on the basis of geographic diversity. The results of these interviews are not generalizable but provide insights.

What GAO Recommends:

- GAO recommends that DHS develop resiliency performance measures, update Protective Security Advisor (PSA) guidelines, and determine the feasibility of developing an approach to disseminate resiliency information.
- DHS is taking action to implement two recommendations and is internally considering the third." [Introductory page]

2.3.2.4 Critical Infrastructure Resilience: Final Report and Recommendations

Title: Critical Infrastructure Resilience: Final Report and Recommendations
Author(s): National Infrastructure Advisory Council (U.S.)
Organization: National Infrastructure Advisory Council
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 54
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf
Date of Publication: September 8, 2009

Objective:

- "The National Infrastructure Advisory Council initiated the Critical Infrastructure Resilience Study to recommend how government and industry can integrate resilience and protection into a comprehensive risk-management strategy. To achieve this, the NIAC sought to identify and address key questions about the role of resilience in the public-private partnership for infrastructure protection." [p. 6]

Scope:

- "This study focuses on critical infrastructure resilience, as opposed to community resilience.
- It also examines how resilience is currently practiced by critical infrastructure businesses and where challenges lie in achieving both enterprise- and sector-level resilience.
- This Study also examines current government policies and programs for resilience in critical infrastructure and key resource (CIKR) sectors. It focuses on identifying measures to achieve sector-and national-level resilience, cross-sector and supply chain related issues as they related to resilience, and measures implemented by individual enterprises." [p. 6]

Description:

- This report presents the key findings of the study, and provides recommendations for strengthening critical infrastructure and key resource sectors.

Additional Information:
These recommendations fall under six categories:

1. "Fortify government policy framework to strengthen critical infrastructure resilience
2. Improve government coordination to enhance critical infrastructure resilience
3. Clarify roles and responsibilities of critical infrastructure partners
4. Strengthen and leverage public-private partnership
5. Encourage resilience using appropriate market incentives
6. Implement government enabling activities & programs in concert with critical infrastructure owners and operators." [p. 2]

2.3.2.5 Critical Infrastructure - Challenges Remain in Protecting Key Sectors

Title: Critical Infrastructure - Challenges Remain in Protecting Key Sectors
Author(s): Eileen R. Larence (Director, Homeland Security and Justice Issues), David A. Powner (Director, Information Technology Management Issues)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 30
Retrieved from: GAO-07-626T, Testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives
Hyperlink: http://www.gao.gov/assets/120/115905.pdf
Date of Publication: March 20, 2007

"Why GAO Did This Study

- As Hurricane Katrina so forcefully demonstrated, the nation's critical infrastructures—both physical and cyber—have been vulnerable to a wide variety of threats. Because about 85 percent of the nation's critical infrastructure is owned by the private sector, it is vital that the public and private sectors work together to protect these assets. The Department of Homeland Security (DHS) is responsible for coordinating a national protection strategy including formation of government and private sector councils as a collaborating tool. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures, in sector-specific plans that comply with DHS's National Infrastructure Protection Plan (NIPP).
- This testimony is based primarily on GAO's October 2006 sector council report and a body of work on cyber critical infrastructure protection. Specifically, it addresses (1) the extent to which these councils have been established, (2) key facilitating factors and challenges affecting the formation of the council, (3) key facilitating factors and challenges encountered in developing sector plans, and (4) the status of DHS's efforts to fulfill key cybersecurity responsibilities.
- GAO has made previous recommendations, particularly in the area of cybersecurity that have not been fully implemented. Continued monitoring will determine whether further recommendations are warranted." [Introductory page]

2.3.2.6 Critical Infrastructure Protections: The 9/11 Commission Report and Congressional Response

Title: Critical Infrastructure Protections: The 9/11 Commission Report and Congressional Response
Author(s): John Moteff, Specialist in Science and Technology Policy - Resources, Science, and Industry Division
Organization: Congressional Research Service (CRS)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 13
Retrieved from: Congressional Research Service Report for Congress, from the Federation of American Scientists website
Hyperlink: http://www.fas.org/sgp/crs/homesec/RL32531.pdf
Date of Publication: Unavailable, but updated January 11, 2005

Description:

- "Federal efforts to protect the nation's critical infrastructure pre-date the September 11, 2001 attacks on the World Trade Center and the Pentagon. Since the attacks, critical infrastructure protection has evolved to include countering that type of an attack. Because the purpose of the Commission's report was to answer, "How did the terrorist attack of September 11, 2001 happen?" and "How can such a tragedy be avoided in the future?," most, if not all, of the recommendations made in the 9/11 Commission's report deal indirectly with critical infrastructure protection. However, there are relatively few recommendations that specifically address critical infrastructure protection.
- This report will identify those recommendations and briefly discuss the possible impacts those recommendations and the subsequent congressional response might have on the nation's efforts to protect its critical infrastructure." [p. 1]

2.3.2.7 Defense Critical Infrastructure - Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure

Title: Defense Critical Infrastructure - Developing Training Standards and an Awareness of Existing Expertise Would Help DOD Assure the Availability of Critical Infrastructure
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 27
Retrieved from: GAO-09-42, Report to Congressional Requesters, from the Government Accountability Office website
Hyperlink: http://www.gao.gov/new.items/d0942.pdf
Date of Publication: October 2008

"Why GAO Did This Study

- The Department of Defense (DOD) relies on a global network of DOD and non-DOD infrastructure so critical that its unavailability could have a debilitating effect on DOD's ability to project, support, and sustain its forces and operations worldwide. DOD established the Defense Critical Infrastructure Program (DCIP) to assure the availability of mission-critical infrastructure.
- GAO was asked to evaluate the extent to which DOD has (1) incorporated aspects of DCIP into its exercises in the Transportation Defense Sector and (2) developed DCIP training standards departmentwide and made installation personnel aware of existing DCIP expertise. GAO examined a nonprojectable sample of 46 critical assets representing the four military services, five combatant commands, and selected installations within five defense sectors. GAO reviewed relevant DOD DCIP guidance and documents and interviewed cognizant officials regarding DCIP exercises, training, and awareness.

What GAO Recommends

- GAO recommends that DOD (1) develop departmentwide DCIP training standards and an implementation time frame and (2) develop an effective means to communicate to installation personnel the existence and availability of DCIP expertise at the combatant command and military service levels. DOD concurred" [Introductory Page]

2.3.2.8 Defense Critical Infrastructure - Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets

Title: Defense Critical Infrastructure - Adherence to Guidance Would Improve DOD's Approach to Identifying and Assuring the Availability of Critical Transportation Assets
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 42
Retrieved from: GAO-08-851, Report to Congressional Requesters
Hyperlink: http://www.gao.gov/assets/280/279681.pdf
Date of Publication: August 2008

"Why GAO Did This Study

- The Department of Defense (DOD) established the Defense Critical Infrastructure Program (DCIP) to assure the availability of mission-critical infrastructure, including surface, sea, and air transportation assets to carry out its missions.
- GAO was asked to evaluate (1) the extent to which the U.S. Transportation Command (TRANSCOM) has identified, prioritized, and assessed critical transportation assets; (2) the extent to which DOD installation personnel have taken actions to help assure the availability of critical transportation assets, both within and independent of DCIP; and (3) how DOD is funding critical transportation asset assurance. GAO examined a nonprojectable sample of 22 critical transportation assets, reviewed relevant DOD guidance and documents, and interviewed cognizant officials.

What GAO Recommends

- GAO recommends TRANSCOM (1) implement established criteria to identify critical transportation assets, and develop a timeline for doing so, (2) discontinue its use of vulnerability assessments as its primary tool for identifying its critical assets, and (3) finalize an agreement with the Joint Staff to participate as transportation experts on Joint Staff DCIP vulnerability assessments, and that the military services develop and implement service-specific DCIP guidance. DOD partially concurred with the recommendations. GAO modified one recommendation on vulnerability assessments, in response to agency comments." [Introductory page]

2.3.2.9 Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets

Title: Defense Critical Infrastructure: DOD's Risk Analysis of Its Critical Infrastructure Omits Highly Sensitive Assets
Author(s): Davi M. D'Agostino (Director, Defense Capabilities and Management)
Organization: United States General Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 20
Retrieved from: GAO-08-373R
Hyperlink: http://www.gao.gov/assets/100/95438.pdf
Date of Publication: April 2, 2008

Description:

- "As part of our ongoing work on DOD's [Department of Defense] critical infrastructure protection efforts, this report focuses on challenges DOD faces in incorporating critical SCI [sensitive compartmented information] and SAP [special access programs] assets into DCIP [defense critical infrastructure program]. Specifically, this report evaluates the extent to which DOD is (1) identifying and prioritizing critical SCI and SAP assets in DCIP and (2) assessing critical SCI and SAP assets for vulnerabilities in a comprehensive manner consistent with that used by DCIP for collateral-level assets." [p. 3]

2.3.2.10 Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure

Title: Defense Infrastructure: Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 48
Retrieved from: GAO-07-461, Report to Congressional Requesters
Hyperlink: http://www.gao.gov/assets/270/261165.pdf
Date of Publication: May 2007

"Why GAO Did This Study

- The Department of Defense (DOD) relies on a network of DOD and non-DOD infrastructure assets in the United States and abroad so critical that its unavailability could hinder DOD's ability to project, support, and sustain its forces and operations worldwide. DOD established the Defense Critical Infrastructure Program (DCIP) to identify and assure the availability of mission-critical infrastructure.
- GAO was asked to evaluate the extent to which DOD has (1) developed a comprehensive management plan to implement DCIP and (2) identified, prioritized, and assessed its critical infrastructure. GAO analyzed relevant DCIP documents and guidance and met with officials from more than 30 DOD organizations that have DCIP responsibilities, and with Department of Homeland Security (DHS) officials involved in protecting critical infrastructure.

What GAO Recommends

- GAO recommends DOD take several actions to improve the efficiency and effectiveness of DCIP operations. Actions include developing a comprehensive management plan; issuing a chartering directive defining the relationship between the directorates responsible for DCIP and antiterrorism missions; and identifying non-DOD-owned critical infrastructure for DHS to consider in its assessments.
- DOD concurred with all of GAO's recommendations." [Introductory page]

2.3.2.11 Cybersecurity - Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems

Title: Cybersecurity - Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems
Author(s): Gregory C. Wilshusen, Director Information Security Issues
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 17
Retrieved from: GAO-11-463T, Testimony before the Subcommittee on Cybersecurity, Infrastructure protection, and Security Technologies, Committee on Homeland Security, House of Representatives
Hyperlink: http://www.gao.gov/assets/130/125786.pdf
Date of Publication: March 16, 2011

"Why GAO Did This Study

- Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of our nation's critical infrastructure and the federal government. In recent testimony, the Director of National Intelligence stated that there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks. In addition, recent reports of cyber attacks and incidents affecting federal systems and critical infrastructures illustrate the potential impact of such events on national and economic security. The nation's ever-increasing dependence on information systems to carry out essential everyday operations makes it vulnerable to an array of cyber-based risks. Thus it is increasingly important that federal and nonfederal entities carry out concerted efforts to safeguard their systems and the information they contain.
- GAO is providing a statement describing (1) cyber threats to cyber-reliant critical infrastructures and federal information systems and (2) the continuing challenges facing federal agencies in protecting the nation's cyber-reliant critical infrastructure and federal systems. In preparing this statement, GAO relied on its previously published work in the area, which included many recommendations for improvements." [Introductory page]

2.3.2.12 Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed

Title: Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 38
Retrieved from: GAO-10-628, Report to Congressional Requesters
Hyperlink: http://www.gao.gov/assets/310/307222.pdf
Date of Publication: July 2010

"Why GAO Did This Study

- Pervasive and sustained computer-based attacks pose a potentially devastating impact to systems and operations and the critical infrastructures they support. Addressing these threats depends on effective partnerships between the government and private sector owners and operators of critical infrastructure. Federal policy, including the Department of Homeland Security's (DHS) National Infrastructure Protection Plan, calls for a partnership model that includes public and private councils to coordinate policy and information sharing and analysis centers to gather and disseminate information on threats to physical and cyber-related infrastructure.
- GAO was asked to determine (1) private sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met and (2) public sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met.
- To do this, GAO conducted surveys and interviews of public and private sector officials and analyzed relevant policies and other documents.

What GAO Recommends:

- GAO recommends that the national Cybersecurity Coordinator and DHS work with their federal and private sector partners to enhance information-sharing efforts. The national Cybersecurity Coordinator provided no comments on a draft of this report.
- DHS concurred with GAO's recommendations." [Introductory Page]

2.3.2.13 Critical Infrastructure Protection - DHS Needs to Better Address Its Cybersecurity Responsibilities

Title: Critical Infrastructure Protection - DHS Needs to Better Address Its Cybersecurity Responsibilities
Author(s): Statement of David Powner, Director, Information Technology Management Issues
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 19
Retrieved from: GAO-08-1157T, Government Accountability Office (GAO)
Hyperlink: http://www.gao.gov/assets/130/121129.pdf
Date of Publication: September 2008

"Why GAO Did This Study

- Recent cyber attacks demonstrate the potentially devastating impact these pose to our nation's computer systems and to the federal operations and critical infrastructures that they support. They also highlight that we need to be vigilant against individuals and groups with malicious intent, such as criminals, terrorists, and nation-states perpetuating these attacks. Federal law and policy established the Department of Homeland Security (DHS) as the focal point for coordinating cybersecurity, including making it responsible for protecting systems that support critical infrastructures, a practice commonly referred to as cyber critical infrastructure protection. Since 2005, GAO has reported on the responsibilities and progress DHS has made in its cybersecurity efforts.
- GAO was asked to summarize its key reports and their associated recommendations aimed at securing our nation’s cyber critical infrastructure.
- To do so, GAO relied on previous reports, as well as two reports being released today, and analyzed information about the status of recommendations.

What GAO Recommends

- GAO has previously made about 30 recommendations to help DHS fulfill its cybersecurity responsibilities and resolve underlying challenges. DHS in large part concurred with GAO’s recommendations and in many cases has actions planned and underway to implement them." [Introductory page]

2.3.2.14 Critical Infrastructure Protection - DHS Needs to Fully Address Lessons Learned from its First Cyber Storm Exercise

Title: Critical Infrastructure Protection - DHS Needs to Fully Address Lessons Learned from its First Cyber Storm Exercise
Author(s): Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 39
Retrieved from: GAO-08-825, Report to Congressional Requesters, from the Government Accountability Office website
Hyperlink: http://www.gao.gov/assets/290/280965.pdf
Date of Publication: September 2008

"Why GAO Did this Study

- Federal policies establish the Department of Homeland Security (DHS) as the focal point for the security of cyberspace. As part of its responsibilities, DHS is required to coordinate cyber attack exercises to strengthen public and private incident response capabilities. One major exercise program, called Cyber Storm, is a large-scale simulation of multiple concurrent cyber attacks involving the federal government, states, foreign governments, and private industry. To date, DHS has conducted Cyber Storm exercises in 2006 and 2008.
- GAO agreed to (1) identify the lessons that DHS learned from the first Cyber Storm exercise, (2) assess DHS's efforts to address the lessons learned from this exercise, and (3) identify key participants' views of their experiences during the second Cyber Storm exercise.
- To do so, GAO evaluated documentation of corrective activities and interviewed federal, state, and private sector officials.

What GAO Recommends:

- GAO is recommending that DHS schedule and complete the corrective activities identified to address lessons learned during the first Cyber Storm exercise, many of which were reiterated during the second Cyber Storm exercise.
- In written comments, DHS agreed with this recommendation and reported on its efforts to complete corrective activities." [Introductory page]

2.3.2.15 Critical Infrastructure Protection - Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks

Title: Critical Infrastructure Protection - Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 27
Retrieved from: GAO-08-607, Report to the Subcommittee on Emerging Threats, Cybersecurity, and science and Technology, Committee on Homeland Security, House of Representatives
Hyperlink: http://www.gao.gov/assets/280/277329.pdf
Date of Publication: June 2008

"Why GAO Did This Study

- Technological advances have led to an increasing convergence of previously separate networks used to transmit voice and data communications. While the benefits of this convergence are enormous, such interconnectivity also poses significant challenges to our nation's ability to respond to major disruptions. Two operations centers—managed by the Department of Homeland Security's (DHS) National Communications System and National Cyber Security Division— plan for and monitor disruptions on voice and data networks. In September 2007, a DHS expert task force made three recommendations toward establishing an integrated operations center that the department agreed to adopt. To determine the status of efforts to establish an integrated center, GAO reviewed documentation, interviewed relevant DHS and private sector officials, and reviewed laws and policies to identify DHS's responsibilities in addressing convergence.

What GAO Recommends

- GAO is recommending that the Secretary of Homeland Security complete (1) its strategic plan and (2) define tasks and milestones for completing remaining integration steps. DHS concurred with GAO's first recommendation. With regard to the second, DHS stated it supports integrating overlapping functions, but does not support merging the centers. However, there is strong evidence supporting the need to merge the centers to enhance incident response." [Introductory Page]

2.3.2.16 Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies

Title: Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies
Author(s): David A. Powner (Director, Information Technology Management Issues)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 14
Retrieved from: GAO-08-64T, Testimony before Congressional Subcommittees, Committee on Homeland Security, U.S. House of Representatives
Hyperlink: http://www.gao.gov/assets/120/118369.pdf
Date of Publication: October 31, 2007

"Why GAO Did This Study

- The nation's critical infrastructure sectors—such as banking and finance, information technology, and public health—rely on computerized information and systems to provide services to the public. To fulfill the requirement for a comprehensive plan, including cyber aspects, the Department of Homeland Security (DHS) issued a national plan in June 2006 for the sectors to use as a road map to enhance the protection of critical infrastructure. Lead federal agencies, referred to as sector-specific agencies, are responsible for coordinating critical infrastructure protection efforts such as the development of plans that are specific to each sector.
- GAO was asked to summarize a report being released today that identifies the extent to which the sector plans addressed key aspects of cyber security, including cyber assets, key vulnerabilities, vulnerability reduction efforts, and recovery plans. In the report, GAO analyzed each sector-specific plan against criteria that were developed on the basis of DHS guidance.

What GAO Recommends

- In its report, GAO recommends that the Secretary of Homeland Security request that, by September 2008, the sector-specific agencies develop plans that fully address all of the cyber-related criteria.
- In written comments on a draft of the report, DHS concurred with GAO's recommendation." [Introductory page]

2.3.2.17 Critical Infrastructure Protection - Challenges in Addressing Cybersecurity

Title: Critical Infrastructure Protection - Challenges in Addressing Cybersecurity
Author(s): David A. Powner (Director, Information Technology Management Issues)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 26
Retrieved from: GAO-05-827T, Testimony before the Subcommittee on Federal Financial Management, Government Information, and International Security, Senate Committee on Homeland Security and Governmental Affairs
Hyperlink: http://www.gao.gov/assets/120/111987.pdf
Date of Publication: July 19, 2005

"Why GAO Did This Study:

- Increasing computer interconnectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures.
- GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve cybersecurity of our nation's critical infrastructure." [Introductory page]

2.3.2.18 Critical Infrastructure Protection - Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities

Title: Critical Infrastructure Protection - Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities
Author(s): United States Government Accountability Office (GAO)
Organization: United States Government Accountability Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 78
Retrieved from: GAO-05-434, Report to Congressional Requesters
Hyperlink: http://www.gao.gov/new.items/d05434.pdf
Date of Publication: May 2005

"Why GAO Did This Study

- Increasing computer interconnectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The Homeland Security Act of 2002 and federal policy established DHS as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures.
- GAO was asked to determine (1) DHS's roles and responsibilities for cyber critical infrastructure protection, (2) the status and adequacy of DHS's efforts to fulfill these responsibilities, and (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities.

What GAO Recommends

- GAO is making recommendations to the Secretary of Homeland Security to strengthen the department's ability to implement key cybersecurity responsibilities by completing critical activities and resolving underlying challenges.
- In written comments on a draft of this report, DHS agreed with our recommendation to engage stakeholders to prioritize its responsibilities, but disagreed with and sought clarification on recommendations to resolve its challenges." [Introductory page]

2.3.2.19 Critical Infrastructure Protection in the National Capital Region: Risk-Based Foundations for Resilience and Sustainability

Title: Critical Infrastructure Protection in the National Capital Region: Risk-Based Foundations for Resilience and Sustainability
Author(s): John E. Bigger and Michael G. Willingham
Organization: University Consortium for Infrastructure Protection
Publisher: George Mason University
Publishing Location: Washington, D.C.
Edition: Unavailable
Pages: 60
Retrieved from: Final Report, Volume 2: Energy Sector, from the Virginia Tech Critical Infrastructure Modeling and Assessment Program (CIMAP) website
Hyperlink: http://www.cimap.vt.edu/2DOC/Vol-02-Energy.pdf
Date of Publication: 2006

Purpose:

- "This report is designed to help the Senior Policy Group (SPG) who represent the state/local public sector, and energy sector personnel of the National Capital Region (NCR) office, to determine vulnerabilities and risks within the energy infrastructure, and to lay the groundwork for a systematic approach to threat and risk evaluation." [p. 3]

Description:

- "A two-fold approach was used to obtain the original energy infrastructure data. First, a literature search was conducted to identify and obtain publicly available documents relating to both energy infrastructure security and vulnerability assessments. Second, energy industry personnel were interviewed to document their organization's activities and experiences related to vulnerability assessments. At each participating organization, interviewers talked with personnel from departments that had participated in the firm's vulnerability assessment and with an executive of the firm who has responsibility for security. A detailed description of the project approach and data collection process is presented in Appendix A." [p. 3]
- This report describes the main findings of the study, and offers recommendations for improving critical infrastructure protection in the energy sector.

2.3.3 United Kingdom

2.3.3.1 The State of the Nation - Infrastructure 2010

Title: The State of the Nation - Infrastructure 2010
Author(s): Institution of Civil Engineers (ICE)
Organization: Institution of Civil Engineers (ICE)
Publisher: Institution of Civil Engineers (ICE)
Publishing Location: Westminster, London, UK
Edition: N/A
Pages: 24
Retrieved from: Institution of Civil Engineers (ICE) website
Hyperlink: http://www.ice.org.uk/getattachment/c198a95f-69bd-4c46-8110-51b057ec20f1/State-of-the-Nation--Infrastructure-2010.aspx
Date of Publication: June 2010

Description:

- This document presents an overview of the Institution of Civil Engineers' (ICE) independent assessment of the state of the UK's infrastructure in 2010. The infrastructure sectors that are assessed in this report are:
  - Energy
  - Strategic Transport Networks
  - Local Transport
  - Water and Wastewater
  - Flood Risk management
  - Waste and Resource Management
- For each of the above sectors, this report describes:
  - condition and capacity;
  - resilience;
  - sustainability;
  - impact of significant cuts; and
  - five year view
- The ICE assigns each sector a grade which summarizes the state of their infrastructures, and provides recommendations for strengthening and protecting them.
- Lastly, the report discusses some key issues which impact the UK's infrastructures. They are:
  - sustainability;
  - capacity and skills;
  - funding and delivery; and
  - planning and regulation

2.3.3.2 The State of the Nation: Defending Critical Infrastructure

Title: The State of the Nation: Defending Critical Infrastructure
Author(s): Institution of Civil Engineers (ICE)
Organization: Institution of Civil Engineers (ICE)
Publisher: Institution of Civil Engineers (ICE)
Publishing Location: Westminster, London, United Kingdom
Edition: Unavailable
Pages: 16
Retrieved from: Institution of Civil Engineers (ICE) website
Hyperlink: http://www.ice.org.uk/getattachment/5e93aedd-3b4c-44db-acfa-d176e0ccbb0e/State-of-the-Nation--Defending-Critical-Infrastruc.aspx
Date of Publication: June 2009

Background:

- "The Institution of Civil Engineers (ICE) has conducted an inquiry into the defence of the UK's critical infrastructure. During the course of our investigation we gathered oral and written evidence from numerous major UK infrastructure asset owners, operators, agencies, service providers and civil engineering consultants and contractors.
- The evidence submitted to ICE by these key industry players has allowed us to produce an independent in-depth assessment of how effectively the UK ensures the resilience of its critical infrastructure." [p. 3]

Description:

- "This report addresses the main threats to our infrastructure: system failure, climate change and terrorism. It explains the current situation and sets out a list of major recommendations to improve the security of our critical infrastructure networks."
  [p. 3]

2.3.3.3 Cyber Security and the UK's Critical National Infrastructure

Title: Cyber Security and the UK's Critical National Infrastructure
Author(s): Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke
Organization: Chatham House
Publisher: Unavailable
Publishing Location: Great Britain
Edition: Unavailable
Pages: 50
Retrieved from: A Chatham House Report, from the Chatham House website
Hyperlink:
http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf
Date of Publication: September 2011

Purpose:

- "There is currently no publicly available, comprehensive account of the UK national cyberspace stakeholder environment that could provide the basis for the development of a national cyber security regime, culture or policy framework. This report aims to fill that gap." [p. vii]

Description:

- "This report asks whether the various agencies, bodies, and individuals involved [in critical infrastructure] recognize the significance of the cyber stakeholder status that has been conferred upon them. How do these organizations identify and measure their cyber dependencies, and how well and systematically do they manage the risks and mitigate the potential vulnerabilities associated with these dependencies?
- The report is based on a series of high-level interviews through which the authors sought to gauge the various organizations' overall understanding of, and response to, the problem of cyber security. Rather than interview communications officers or representatives of IT departments, the authors sought wherever possible to assess the level of cyber security awareness at board level, and particularly among the most senior executives who had no specific IT expertise. " [p. vii]
- This document presents the findings of this study, and offers policy recommendations for collaboration between the private and public sectors.

Additional Information:
This report covers the following topics:

- "Perceptions and the Threat Landscape;
- Managing Cyber Dependencies;
- Information Communications and Outreach; and
- Building Cyber Security Culture." [p. 3-4]

2.3.3.4 Ireland at Risk: Critical Infrastructure - Adaptation for Climate Change

Title: Ireland at Risk: Critical Infrastructure - Adaptation for Climate Change
Author(s): Irish Academy of Engineering
Organization: Irish Academy of Engineering
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 37
Retrieved from: Based on presentations and discussions at a symposium convened by the Academy of Engineering in Dublin in April 2009
Hyperlink: http://www.iae.ie/site_media/pressroom/documents/2009/Nov/17/Ireland_at_Risk_2.pdf
Date of Publication: 2009

Description:

- "This report outlines how best to proceed to meet the challenge of adapting our infrastructure for climate change." [p. 5]
- First, it describes three key vulnerabilities affecting critical infrastructure. They are:
  - Water supplies
  - Flood protection
  - Energy supplies.
- The report then describes the impacts that climate change can have on critical infrastructure vulnerabilities.
- Lastly, the report provides recommendations for adapting Northern Ireland's infrastructure to climate change.

2.3.4 Australia

2.3.4.1 Resilience in the Australian Food Supply Chain

Title: Resilience in the Australian Food Supply Chain
Author(s): Sapere Research Group
Organization: Prepared for the Australian Government, Department of Agriculture, Fisheries and Forestry
Publisher: Australian Government, Department of Agriculture, Fisheries and Forestry
Publishing Location: Australia
Edition: Unavailable
Pages: 83
Retrieved from: Australian Government, Department of Agriculture, Fisheries and Forestry website
Hyperlink: http://www.daff.gov.au/__data/assets/pdf_file/0009/1915290/resilience-food-supply.pdf
Date of Publication: February 2012

Background:

- This is the second of two studies conducted by the Sapere Research Group (SRG) regarding food supply chain resilience. This second study was initiated in response to the floods of December 2010 and January 2011, which severely tested Australian food supply chains.
- This study involved interviews and surveys of a large cross section of the Australian food industry.

Description:

- This report presents the findings of the Sapere Research Group's study.
- The key question that underlies this study is "whether, following a natural disaster or other major disruptive event, Australians in affected regions would go hungry." [p. vi]
- This study identified several new issues and risks which must be addressed in order to improve the resilience of the food supply chain. These include: "the vital role played by communications networks; the risks associated with concurrent disaster events; and the need for greater understanding, especially among younger and/or socially vulnerable consumers, of alternative food sources and cooking methods." [p. vii]

Additional Information:
This report includes the following sections:

- Summary
- Introduction
- Overview of Australia's food supply chain
- Possible threats to food supply chain resilience
- Lessons from the 2010-11 floods in Queensland
- Emerging challenges to food supply chain resilience
- Key areas for further investigation and possible action
- Appendix 1: Terms of reference
- Appendix 2: Case studies
- Appendix 3: Queensland flood review

2.3.4.2 Which Organisational Model Meets Best Practice Criterion for Critical Infrastructure Providers: An Examination of Infrastructure Providers: An Examination of the Australian Perspective Based on Case Studies

Title: Which Organisational Model Meets Best Practice Criterion for Critical Infrastructure Providers: An Examination of Infrastructure Providers: An Examination of the Australian Perspective Based on Case Studies
Author(s): Andrew Woodward and Craig Valli
Organization: Security Research Centre, School of Computer and Security Science, Edith Cowan University (Perth, Western Australia)
Publisher: Edith Cowan University
Publishing Location: Perth, Western Australia
Edition: N/A
Pages: 7
Retrieved from: Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University (August 23rd 2010)
Hyperlink: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1014&context=icr&sei-redir=1&referer=http%3A%2F%2Fwww.google.ca%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Duk%2520best%2520practice%2520and%2520existing%2520standard%2520reports%2520for%2520critical%2520infrastructure%26source%3Dweb%26cd%3D8%26ved%3D0CF8QFjAH%26url%3Dhttp%253A%252F%252Fro.ecu.edu.au%252Fcgi%252Fviewcontent.cgi%253Farticle%253D1014%2526context%253Dicr%26ei%3D2uj-T7f8Gqbz0gGKp4HOBg%26usg%3DAFQjCNHfVvY0OyYSAWrd_qXVLZTay2K7Hw#search=%22uk%20best%20practice%20existing%20standard%20reports%20critical%20infrastructure%22
Date of Publication: 2010

Abstract
"While it is recognised that there must be segregation between corporate and process control networks in order to achieve a higher level of security, there is evidence that this is not occurring. Computer and network vulnerability assessments were carried out on three Australian critical infrastructure providers to determine their level of security. The security measures implemented by each organisation have been mapped against best practice recommendations for achieving segregation between process control and corporate networks. One of the organisations used a model which provided a dedicated information security team for provision of security for the process control networks. One of the other organisations relied heavily on outsourcing for their IT security, and a third used in house corporate IT for their process control security. It was found that the organisation using a dedicated IT security team that worked within the process control group achieved the highest level of security when mapped to best practice. This paper concludes that best practice recommendations for critical infrastructure providers should also include guidelines for the organisational structure, and further, that dedicated IT security personnel be placed within the process control group." [p. 118]

Keywords: SCADA security; critical infrastructure protection; organisational model; operational technology; information technology

2.3.5 Multi/International

2.3.5.1 The Challenges for European Critical Infrastructure Protection

Title: The Challenges for European Critical Infrastructure Protection
Author(s): Christer Pursiainen (Council of the Baltic Sea States Secretariat, Strömsborg, Stockholm, Sweden)
Organization: Unavailable
Publisher: Routledge
Publishing Location: Unavailable
Edition: N/A
Pages: 721-739
Retrieved from: European Integration, Vol. 31, No. 6
Hyperlink: N/A
Date of Publication: November 2009

Abstract:
"Critical Infrastructure Protection has become a new field of European integration. This article identifies some of the challenges on this road towards a more shared approach. It argues that while the very concept of critical infrastructure is in flux, the whole approach is challenged by the more general approach that concentrates on resilience of societal functions instead of mere protection of infrastructures. The article also claims that it is not completely clear against what kind of threats the critical infrastructures should be protected and by whom. The article further points out the limits of the regulatory efforts of the governments or the EU in trying to protect infrastructures that are mostly owned and operated by private actors." [p. 721]

Key Words: European Programme for Critical Infrastructure Protection (EPCIP); critical infrastructures; resilience; public–private partnership; terrorism; civil protection

2.3.5.2 In the Dark - Crucial Industries Confront Cyberattacks

Title: In the Dark - Crucial Industries Confront Cyberattacks
Author(s): Stewart Baker, Natalia Filipiak, Katrina Timlin
Organization: McAfee and the Center for Strategic and International Studies (CSIS)
Publisher: McAfee
Publishing Location: Unavailable
Edition: Unavailable
Pages: 28
Retrieved from: McAfee second annual critical infrastructure protection report
Hyperlink: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf
Date of Publication: 2011

Description:

- For this report, survey data, research, and interviews were used to obtain a detailed picture of cyber risks in 14 countries.
- This report provides an overview of the risk environment for cyber attacks by describing the threats and vulnerabilities, responses to cyber threats, as well as recommendations for improving security.
- The report focused on critical civilian infrastructures that depend most heavily on industrial control systems. Hence, this report focuses on power, oil, gas and water sectors, as they may be the first targets for a serious cyber attack.

Additional Information:
This report includes the following sections:

- Introduction and Summary
- Threats and Vulnerabilities are Accelerating
- Incremental Response to Cyberthreats
- Government Response
- Recommendations
- Conclusion
- Acknowledgements

2.3.5.3 In the Crossfire - Critical Infrastructure in the Age of Cyber War

Title: In the Crossfire - Critical Infrastructure in the Age of Cyber War
Author(s): Stewart Baker, Shaun Waterman, George Ivanov
Organization: McAfee, Center for Strategic and International Studies (CSIS)
Publisher: McAfee
Publishing Location: Unavailable
Edition: Unavailable
Pages: 44
Retrieved from: McAfee website
Hyperlink: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf
Date of Publication: 2009

Description:

- This report is based on the results of an anonymous and detailed survey which was completed by six hundred IT and security executives from critical infrastructure enterprises. The survey spanned across 7 sectors and 14 countries all over the world.
- The participants were asked questions about their "practices, attitudes and policies on security - the impact of regulation, their relationship with government, specific security measures employed on their networks, and the kinds of attacks they face." [p. 1]
- This report "paints a detailed picture of the way those charged with the defense of critical IT networks are responding to cyber attacks, attempting to secure their systems and working with governments." [p. 1].
- It also provides a comparison of security in different sectors and nations.

Additional Information:
This report includes the following sections:

- Introduction
- The Threat is Real
- Responding to the Threat - Resources and Preparedness
- Countering the Threat - Security Measures
- The "State of Nature" and the Role of Government
- Improving Security in an Age of Cyber War
- Acknowledgements

2.3.5.4 Cybersecurity and Critical Infrastructure Protection

Title: Cybersecurity and Critical Infrastructure Protection
Author(s): James A. Lewis
Organization: Center for Strategic and International Studies
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 12
Retrieved from: Center for Strategic and International Studies website
Hyperlink: http://csis.org/files/media/csis/pubs/0601_cscip_preliminary.pdf
Date of Publication: January 2006

Description:

- This paper argues that computer networks are vulnerable, but that "the cyber threat to critical infrastructure has been overstated, particularly in the context of terrorism." [p. 1]
- However, this does not mean that cybersecurity should be ignored when planning for critical infrastructure protection planning. Vulnerabilities increase as the use of computer networks grows. In addition, more sophisticated opponents can use network attacks to target the information stored within computer networks. This is a different kind of threat from what was originally envisioned, and addressing it may require a reorientation of our approach to cybersecurity.
- This chapter discusses the reasons and goals for rethinking cybersecurity for critical infrastructure.

Additional Information:
This paper includes the following sections:

- Political Context for Cybersecurity and Critical Infrastructure Protection
- Assessing risk
- Computer Networks and Critical Infrastructures
- The Internet as a Critical Infrastructure

3 Processes for Managing CI

Overview

This chapter presents references which provide methodologies, tools, approaches, or discussions regarding the various processes involved in critical infrastructure (CI) management. While Chapter 2 presented high-level documents, the references in this chapter provide more detail on specific processes for CI management. Most of these references are not country-specific, although some describe a country's approach or methodology for one of the components of the CI management process. These references are divided into the following sections:

- Section 3.1: Identifying CI
- Section 3.2: Risk and vulnerability analysis of CI
- Section 3.3: Understanding CI systems, their interdependencies, and how they play out in disaster scenarios
- Section 3.4: Protecting CI
- Section 3.5: Responding to and recovering from disruptions to CI
- Section 3.6: Clarifying roles and improving collaboration
  This Section is further divided according to the subject area. They are: roles and responsibilities; and information sharing.

Similar references are grouped, and then ordered chronologically from most recent to least recent.

3.1 Identifying CI

3.1.1 Critical Infrastructure Rating Workbook

Title: Critical Infrastructure Rating Workbook
Author(s): Provincial Emergency Program (PEP), Emergency Management British Columbia (EMBC)
Organization: Provincial Emergency Program (PEP), Emergency Management British Columbia (EMBC)
Publisher: Provincial Emergency Program (PEP), Emergency Management British Columbia (EMBC)
Publishing Location: Unavailable
Edition: Freshet Pilot Version 2
Pages: 37
Retrieved from: Provincial Emergency Program (PEP) website
Hyperlink: http://www.pep.bc.ca/community/CI-RatingsWkbk.pdf
Date of Publication: May 2007

Purpose:

- "The purpose of the Critical Infrastructure Rating Workbook is:
  To assist municipalities, industries and communities, in identifying and rating their Critical Infrastructure (CI) Assets within a defined geographic area that may be at risk from a hazardous event." [p. 1]

Objective:

- "The workbook has been designed to be used for the rating of CI assets by the owners under all hazards and threats. However, its first use will be under the hazardous event of potential flooding within British Columbia (Freshet 2007). The objective of the rating is for the emergency planners and asset owners to identify the CI assets which may be at most risk and to help provide information for those in developing possible solutions to protect and minimize damage to these facilities." [p. 1]

Additional Information:

- This workbook guides users through a 5-step process for rating critical infrastructure. They are:
  1) Identification of critical infrastructure assets
  2) Rating of critical infrastructure assets
  3) Determining dependencies of critical infrastructure assets
  4) Exposure assessment
  5) Submission and Consultation
- For each of the above tasks, the workbook provides guidance on: the process (including task strategies and required information), the procedure (including steps and examples), and results.

3.1.2 Infrastructure Taxonomy

Title: Infrastructure Taxonomy
Author(s): Infrastructure Information Collection Division (IICD), Office of Infrastructure Protection, Department of Homeland Security
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: Unavailable
Edition: Version 3
Pages: 264
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: November 1, 2008

Description:

- "Since the Department of Homeland Security must interface with a wide range of infrastructure operators; commercial and industrial owners; and federal, state, and local agencies, it is important to adopt a taxonomy (or structure) that facilitates effective communication.
- This document outlines the taxonomy used by DHS to categorize various infrastructure elements. To the extent possible, the terminology is representative of each industry. It should be noted that the taxonomy used here is not intended to displace the common industry 'jargon.' Rather, it is intended to describe what DHS means when a specific term is used. Further, the taxonomy is not intended to provide any qualification or level of criticality or significance. The taxonomy merely defines the mutually exclusive categories to outline all infrastructure types within a given sector." [p. 1]

Additional Information:

- "Infrastructure assets are first grouped into broad infrastructure sectors (e.g. Agriculture and Food, Energy, Transportation Systems) and then categorized in more detail as needed. Up to five levels of detail are used, although not all assets require all five levels. These levels, in descending order, are the sector, subsector, segment, sub segment, and asset type." [p. 1]
- This taxonomy has two parts:
    - Table 1: reference of the taxonomy categories
    - Annex A: Detailed taxonomy, which includes
        1. "Brief description of each category;
        2. The North American Industry Classification System (NAICS) code that applies, where applicable; and
        3. A set of attributes for each category that can be used to further characterize an asset. The list of attributes provides a relative sample and is by no means all-inclusive." [p. 1]

3.1.3 Critical Infrastructure and Key Assets: Definition and Identification

Title: Critical Infrastructure and Key Assets: Definition and Identification
Author(s): John Moteff and Paul Parfomak (Resources, Science, and Industry Division)
Organization: Congressional Research Service
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 19
Retrieved from: Congressional Report Service (CRS) Report for Congress, from the Federation of American Scientists (FAS) website
Hyperlink: http://www.fas.org/sgp/crs/RL32631.pdf
Date of Publication: October 1, 2004

Description:

- "This report reviews the concept and definition of "critical infrastructure" as it has appeared in federal reports, legislation and regulation since the early 1980s. The report highlights the changes and expansion of that definition as the focus of public policy debates shifted from infrastructure adequacy to infrastructure protection. Finally the report summarizes current policy issues associated with critical infrastructure identification by federal agencies and the private sector. The report is intentionally limited to definitional issues and categorization of infrastructure. For a more general discussion of national policy regarding critical infrastructure protection, including its evolution, implementation, and continuing issues, see CRS Report RL30153, Critical Infrastructures: Background, Policy, and Implementation." [p. 1]

3.1.4 Critical Infrastructures: What Makes an Infrastructure Critical?

Title: Critical Infrastructures: What Makes an Infrastructure Critical?
Author(s): John Moteff, Claudia Copeland, and John Fischer (Resources, Science, and Industry Division)
Organization: Congressional Research Service (CRS)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 20
Retrieved from: Congressional Research Service, Report for Congress, from the Federation of American Scientists (FAS) website
Hyperlink: http://www.fas.org/irp/crs/RL31556.pdf
Date of Publication: August 30, 2002, updated January 29, 2003

Description:

- This paper "recounts how the definition [of critical infrastructure] (and the list of illustrative examples) has broadened over time and what impact this may have on developing and implementing critical infrastructure protection policy." [p. 1]

Additional Information:
This document contains the following sections:

- "Introduction
- Background
  - What is a Critical Infrastructure?
  - Which Assets of a Critical Infrastructure Need Protection?
  - Surface Transportation: River Crossings
  - Transportation Systems: Air Traffic Control (ATC)
  - Observations
- Analysis
- Appendices:
  - What is Infrastructure?
  - How the Criteria and Components of Critical Infrastructure Have Expanded Over Time" [Table of Contents]

3.1.5 CARVER + Shock Primer for Food Sector Vulnerability Assessments

Title: CARVER + Shock Primer for Food Sector Vulnerability Assessments
Author(s): Unavailable
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 13
Retrieved from: University of Tennessee, Institute of Agriculture website
Hyperlink: http://www.vet.utk.edu/cafsp/resources/pdf/CARVER%20plus%20Shock%20Primer.pdf
Date of Publication: Unavailable

Description:

- This document provides a description of the CARVER plus Shock method. This method is a tool used in the food sector for identifying and prioritizing the targets that are most susceptible to attack.
- This document includes:
  - "Steps for Conducting a CARVER + Shock Analysis" [p. 3]
  - "Description of Attributes and Scales" [p. 4]
  - "Calculation of Final Values and Interpretation" [p. 7]
  - Appendices, which include worksheets and summary tables used in conducting the assessment

3.1.6 Mission Critical Business Units, and "Person Criticality" - How Is This Determined? (Electricity Sector)

Title: Mission Critical Business Units, and "Person Criticality" - How Is This Determined? (Electricity Sector)
Author(s): Unavailable
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Australia
Edition: Unavailable
Pages: 19
Retrieved from: Trusted Information Sharing Network website
Hyperlink: http://www.tisn.gov.au/Documents/Criticality+Spreadsheet+-+Electricity+Sector.pdf
Date of Publication: Unavailable

Background:

- "The business unit is valuable to the business and its services delivery. This business unit needs to be ranked in importance against the rest of the business for it to survive any catastrophe affecting its personnel.
- The key people that keep this business unit running need to be ranked within that business unit and identified and compared in the view of a loss of that persons for an extended period of time." [p. 1]

Description:

- This template is a tool that can be used by businesses in the electricity sector to determine the business units and people that are most critical to ensuring continuity of business operations. It is an excel-based worksheet, and is accompanied by a document which provides explanations and guidance on using the template.
- The template is divided according to business units. They are as follows:
    - Corporate Support
    - Network Engineering Support
    - Network Field Services
    - Transmission (Asset Management)
    - Electricity Distribution Maintenance
    - Network Planning
    - Generation
    - Generating Plant Fuel Supply
    - Alternative Fuel Supply
    - Retail and Customer Services
    - System Control
    - Finance
    - Purchasing
    - IT Services
    - Corporate management, including the Disaster Management Team
    - Human Resources, Industrial Relations & Safety
    - Spare sheet for Services #1

3.1.7 Business Unit Criticality, and Person Criticality - How Is This Worked Out?

Title: Business Unit Criticality, and Person Criticality - how is this worked out?
Author(s): Unavailable
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Australia
Edition: Unavailable
Pages: 25
Retrieved from: Trusted Information Sharing Network (TISN) website
Hyperlink: http://www.tisn.gov.au/Documents/Criticality+Spreadsheet+-+Gas+and+Liquid+Fuels+Sector.pdf
Date of Publication: Unavailable

Background:

- "The business unit is valuable to the business and its services delivery. This business unit should be ranked against the rest of the business for it to survive any catastrophe affecting its personnel.
- The key people that keep this business unit running need to be ranked within that business unit and identified and compared in the view of a loss of that persons for an extended period of time." [p. 1]

Description:

- This template is a tool which allows businesses in the gas and liquid fuels sector to identify which business units and people are most critical to ensuring continuity of operations. It is an excel-based worksheet, and is accompanied by a document which provides explanations for using the template.
- The template is divided into business units. They are :
    - Business and Corporate Support
    - Downstream Oil Shipping
    - Refining
    - Storage and Distribution
    - Oil Retail Operations
    - Aviation Fuels
    - Business General Management, Disaster Recovery

3.1.8 A Risk-Based Approach for Identifying Key Economic and Infrastructure Systems

Title: A Risk-Based Approach for Identifying Key Economic and Infrastructure Systems
Author(s): Kash Barker and Joost R. Santos
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 962-974
Retrieved from: Risk Analysis, Vol. 30, No. 6
Hyperlink: N/A
Date of Publication: June 2010

Abstract:
"This article introduces approaches for identifying key interdependent infrastructure sectors based on the inventory dynamic inoperability input-output model, which integrates an inventory model and a risk-based interdependency model. An identification of such key sectors narrows a policymaker's focus on sectors providing most impact and receiving most impact from inventory-caused delays in inoperability resulting from disruptive events. A case study illustrates the practical insights of the key sector approaches derived from a value of workforce-centered production inoperability from Bureau of Economic Analysis data." [p. 962]

Key words: Decision making; input-output analysis; interdependent systems; inventory; key sector analysis; preparedness

3.1.9 A Methodology for the Identification of Critical Locations in Infrastructures

Title: A Methodology for the Identification of Critical Locations in Infrastructures
Author(s): Douglas M. Lemon
Organization: Massachusetts Institute of Technology
Publisher: Massachusetts Institute of Technology
Publishing Location: Massachusetts, United States of America
Edition: N/A
Pages: 113
Retrieved from: Thesis submitted to the Department of Nuclear Engineering on April 30, 2004 in partial fulfillment of the requirements for the Degree of Master Science in Nuclear Engineering
Hyperlink: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA426227
Date of Publication: April 2004

Abstract:
"The extreme importance of critical infrastructures to modern society is widely recognized. These infrastructures are complex, interdependent, and ubiquitous; they are sensitive to disruptions that can lead to cascading failures with serious consequences. Protecting the critical infrastructures from terrorism, human generated malevolent attack directed toward maximum social disruption, presents an enormous challenge. Recognizing that society cannot afford the costs associated with absolute protection, it is necessary to identify the critical locations in these infrastructures. By protecting the critical locations society achieves the greatest benefit for the protection investment. This project examines a screening methodology for the identification of critical locations in infrastructures. The framework models the infrastructures as interconnected digraphs and employs graph theory and reliability theory to identify the vulnerable points. The vulnerable points are screened for their susceptibility to a terrorist attack, and a prioritized list of critical locations is produced. The prioritization methodology is based on multi-attribute utility theory, and involves various disciplines including quantitative risk assessment and decision analysis. The methodology is illustrated through the presentation of a portion on the analysis conducted on the community of the Massachusetts Institute of Technology." [p. 2]

3.2 Risk and Vulnerability Analysis for CI

3.2.1 An All-Hazard Approach for the Vulnerability Analysis of Critical Infrastructures

Title: An All-Hazard Approach for the Vulnerability Analysis of Critical Infrastructures
Author(s): E. Zio, R. Iccinelli and G. Sansavini
Organization: Unavailable
Publisher: ESREL 2011
Publishing Location: Troyes, France
Edition: Version 1
Pages: 8
Retrieved from: Conference Paper from ESREL 2011, Troyes: France
Hyperlink: http://hal-ecp.archives-ouvertes.fr/docs/00/65/80/98/PDF/anno_2011_11.pdf
Date of Publication: September 2011

Abstract:
"In this paper, a framework is proposed for the All-HAZard ANalysis (A-HAZAN) of Critical Infrastructures (CIs). Starting from the identification of the task of each component in the infrastructure, we use tabular procedures to organize the information on the susceptibility to attacks, to single and cascading failures. All variables and states are identified that may impact on the component's role as a possible source of vulnerability within the CI and towards interdependent CIs. This is a starting point for a quantitative evaluation of the degree of exposure to intentional acts. A case study of literature is taken as an exemplary demonstration of the procedures of the analysis." [p. 1]

3.2.2 State-Wide Natural Hazard Risk Assessment - Report 4: Critical Public Infrastructure- An Analysis of Exposure to Natural Hazards

Title: State-Wide Natural Hazard Risk Assessment - Report 4: Critical Public Infrastructure- An Analysis of Exposure to Natural Hazards
Author(s): Risk Frontiers
Organization: Prepared for Queensland Department of Community Safety
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: 78
Retrieved from: Queensland Government Disaster Management Website
Hyperlink: http://www.disaster.qld.gov.au/Disaster%20Resources/Documents/Report%204.pdf
Date of Publication: May 2011

Purpose:
"The main aim of this part of the project was to:

- provide a methodology for determining spatially explicit risk ratings for each type of infrastructure (i.e. point and linear feature);
- determining risk ratings for each infrastructure point and linear infrastructure feature in relation to hazard layers (bushfire, coastal hazards and tropical cyclone winds);
- reporting strategic results at LGA [local government authority] level; and
- make data available to DCS [Department of Community Safety] in a format that facilitates future analysis, reporting and updating." [p. 3]

Description:

- "This report describes the natural hazard risk of public infrastructure in terms of its location and thus exposure to natural hazards. The analysis has been conducted by identifying and mapping infrastructure's level of exposure to bushfire, coastal hazards, floods and tropical cyclone winds... The comprehensive investigation uses infrastructure GIS data provided by the Department of Community Safety (DCS), including major critical infrastructure and social infrastructure." [p. 3]

Additional Information:
This document includes:

- Classification tables for critical infrastructure
- Infrastructure data on public buildings, other point-based infrastructure, roads, and other linear infrastructure
- Description of the analysis methods that were used to determine spatially relevant risk ratings for critical infrastructure. Hazards considered are bushfire, coastal hazards, and tropical cyclone winds.
- Overview of the results: Identification of critical infrastructure that is at risk from each of the above hazards

3.2.3 Risk Analysis for Critical Asset Protection

Title: Risk Analysis for Critical Asset Protection
Author(s): William L. McGill, Bilal M. Ayyub, and Mark Kaminsky
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 1265-1281
Retrieved from: Risk Analysis: An International Journal, Vol. 27, Issue 5
Hyperlink: N/A
Date of Publication: October 2007

Abstract:
"This article proposes a quantitative risk assessment and management framework that supports strategic asset-level resource allocation decision making for critical infrastructure and key resource protection. The proposed framework consists of five phases: scenario identification, consequence and criticality assessment, security vulnerability assessment, threat likelihood assessment, and benefit-cost analysis. Key innovations in this methodology include its initial focus on fundamental asset characteristics to generate an exhaustive set of plausible threat scenarios based on a target susceptibility matrix (which we refer to as asset-driven analysis) and an approach to threat likelihood assessment that captures adversary tendencies to shift their preferences in response to security investments based on the expected utilities of alternative attack profiles assessed from the adversary perspective. A notional example is provided to demonstrate an application of the proposed framework. Extensions of this model to support strategic portfolio-level analysis and tactical risk analysis are suggested." [p. 1265]

Key Words: Consequence; critical asset protection; decision; homeland security; risk analysis; security; terrorism; threat assessment; vulnerability

3.2.4 Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors

Title: Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors
Author(s): Chenyang Lian, Joost R. Santos, and Yacov Y. Haimes
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 1053-1064
Retrieved from: Risk Analysis, Vol. 27, No. 4
Hyperlink: N/A
Date of Publication: August 2007

Abstract:
"Willful attacks or natural disasters pose extreme risks to sectors of the economy. An extreme-event analysis extension is proposed for the Inoperability Input-Output Model (IIM) and the Dynamic IIM (DIIM), which are analytical methodologies for assessing the propagated consequences of initial disruptions to a set of sectors. The article discusses two major risk categories that the economy typically experiences following extreme events: (i) significant changes in consumption patterns due to lingering public fear and (ii) adjustments to the production outputs of the interdependent economic sectors that are necessary to match prevailing consumption levels during the recovery period. Probability distributions associated with changes in the consumption of directly affected sectors are generated based on trends, forecasts, and expert evidence to assess the expected losses of the economy. Analytical formulations are derived to quantify the extreme risks associated with a set of initially affected sectors. In addition, Monte Carlo simulation is used to handle the more complex calculations required for a larger set of sectors and general types of probability distributions. A two-sector example is provided at the end of the article to illustrate the proposed extreme risk model formulations." [p. 1053]

3.2.5 Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework

Title: Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework
Author(s): Bilal M. Ayyub, William L. McGill, and Mark Kaminskiy
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 789-801
Retrieved from: Risk Analysis, Vol. 27, No. 4
Hyperlink: N/A
Date of Publication: August 2007

Abstract:
"This article develops a quantitative all-hazards framework for critical asset and portfolio risk analysis (CAPRA) that considers both natural and human-caused hazards. Following a discussion on the nature of security threats, the need for actionable risk assessments, and the distinction between asset and portfolio-level analysis, a general formula for all-hazards risk analysis is obtained that resembles the traditional model based on the notional product of consequence, vulnerability, and threat, though with clear meanings assigned to each parameter. Furthermore, a simple portfolio consequence model is presented that yields first-order estimates of interdependency effects following a successful attack on an asset. Moreover, depending on the needs of the decisions being made and available analytical resources, values for the parameters in this model can be obtained at a high level or through detailed systems analysis. Several illustrative examples of the CAPRA methodology are provided." [p. 789]

Key Words: All hazards; consequence; critical asset protection; decision; homeland security; risk analysis; security; terrorism; threat; vulnerability

3.2.6 Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences

Title: Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences
Author(s): John Moteff (Specialist in Science and Technology Policy: Resources, Science, and Industry Division)
Organization: Congressional Research Service (CRS)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 29
Retrieved from: Congressional Research Service (CRS) Report for Congress, retrieved through the Federation of American Scientists (FAS) website
Hyperlink: http://www.fas.org/sgp/crs/homesec/RL32561.pdf
Date of Publication: Updated February 4, 2005

Background:

- The Information Analysis and Infrastructure Protection (IA/IP) Directorate has been assigned many duties associated with "coordinating the nation's efforts to protect its critical infrastructure… In particular, the IA/IP Directorate is to integrate threat assessments with vulnerability assessments in an effort to identify and manage the risk associated with possible terrorist attacks on the nation's critical infrastructure. By doing so, the Directorate is to help the nation set priorities and take cost-effective protective measures." [p. 1]

Description:

- "This report is meant to support congressional oversight by discussing, in more detail, what this task entails and issues that need to be addressed. In particular, the report defines terms (e.g. threat, vulnerability, and risk), discusses how they fit together in a systematic analysis, describes processes and techniques that have been used to assess them, and discusses how the results of that analysis can inform resource allocation and policy.
- While the IA/IP Directorate has been given this task as one of its primary missions, similar activities are being undertaken by other agencies under other authorities and by the private sector and states and local governments. Therefore, this report also discusses the Department's role in coordinating and/or integrating these activities." [p. 1]

3.2.7 A Risk Assessment Methodology for Critical Transportation Infrastructure

Title: A Risk Assessment Methodology for Critical Transportation Infrastructure
Author(s): Y.Y. Haimes, J.H. Lambert, S. Kaplan, I. Pikus, and F. Leung
Organization: Center for Risk Management of Engineering Systems, University of Virginia
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 62
Retrieved from: Final Contract Report Sponsored by Virginia Transportation Research Council
Hyperlink: http://ntl.bts.gov/lib/19000/19100/19177/PB2002104760.pdf
Date of Publication: March 2002

Abstract:
"The U.S. transportation system is vulnerable and "open" to many risks, which can be categorized broadly as natural, accidental, and willful. The system traditionally has been protected against natural and accidental events but not against willful hazard. With the exception of civil aviation and the port system, few measures are currently in place in the transportation system to counter threats of terrorism (President's Commission on Critical Infrastructure Protection 1997; National Research Council 1999).

Infrastructure protection typifies a problem of risk assessment and management in a large-scale system. This study offers a methodological framework to identify, prioritize, assess, and manage risks. It includes the following major considerations: (1) a holistic approach to risk identification; (2) prioritization of a large number of risks or risk scenarios; (3) structured solicitation and effective integration of expert judgment into qualitative and quantitative analyses to supplement limited data availability; (4) extreme and catastrophic event analysis; and (5) use of multiobjective framework to evaluate management options (i.e., analyzing trade-offs among noncommensurate, conflicting objectives such as risk and cost). The methodology was illustrated using five case studies of selected transportation infrastructures in the Commonwealth of Virginia." [p. vii]

Key words: Risk; assessment; protection; critical infrastructure

3.2.8 Are We Forgetting the Risks of Information Technology?

Title: Are We Forgetting the Risks of Information Technology?
Author(s): Thomas A. Longstaff, Clyde Chittister, Rich Pethia, Yacov Y. Haimes
Organization: IEEE
Publisher: IEEE Computer Society Press
Publishing Location: Los Alamitos, CA
Edition: N/A
Pages: 43-51
Retrieved from: Computer, Vol. 33, Issue 12
Hyperlink: N/A
Date of Publication: December 2000

Abstract:
"The emerging dominance of software in the lifecycle of our information systems, coupled with the risk and uncertainty associated with its development and maintenance, are increasing information systems vulnerability. Global interconnected-ness through the Internet and the increasing use of supervisory control and data acquisition systems to remotely operate the critical infrastructure through the telecommunications network have rendered our information systems more vulnerable to intrusion and the transmission of malicious misinformation and signals. For all practical purposes, international boundaries have been eliminated in cyber-space. The growth of information technology and almost universal access to computers have enabled hackers and would-be terrorists to attack information systems and critical infrastructures worldwide. The authors describe the hierarchical holographic modeling framework, which promotes a systemic process for assessing risk to critical infrastructures"[6]

[6]From
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=889092&contentType=Journals+%26+Magazines&searchField%3DSearch_All%26queryText%3Dare+we+forgetting+the+risks+of+information+technology

3.2.9 Risk Assessment Methodologies for Critical Infrastructure Protection. Part 1: A State of the Art

Title: Risk Assessment Methodologies for Critical Infrastructure Protection. Part 1: A State of the Art
Author(s): Georgios Giannopoulos. Roberto Filippini, Muriel Schimmer
Organization: Joint Research Centre (JRC) and the Institute for the Protection and Security of the Citizen (IPSC)
Publisher: Publications Office of the European Union
Publishing Location: Luxembourg
Edition: Unavailable
Pages: 53
Retrieved from: Joint Research Centre (JRC) Technical Notes, from the European Commission website
Hyperlink: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf
Date of Publication: 2012

Purpose:

- "The aim of the present report is to obtain a structured review of the existing methodologies at EU and global level, identify gaps and prepare the ground for the proposal of a risk assessment methodology at European level. The aim is not to establish a new methodology from scratch but rather build on existing knowledge in Europe and worldwide so that it will be suitable for European critical infrastructures risk assessment needs." [p. 8]

Description:
This report includes:

- An overview of existing policies in the European Union and worldwide;
- A theoretical introduction to risk assessment methodologies;
- Review of selected methodologies;
- Gap analysis on elements that are missing at a global level, with a special emphasis on Europe; and
- Summary table of methodologies

Additional Information:
"In order to obtain a structured review, the evaluation of these methodologies took place according to the following criteria:

- Scope of the methodology: Which sector is addressed, to whom it is addressed (Policy makers, researchers, operators etc.)
- Objectives of the methodology.
- Interdependencies coverage.
- Is resilience addressed?
- If cross-sectoral methodology, how are risks compared across sectors?" [p. 8-9]

3.2.10 Critical Infrastructure Protection: Elements of Risk

Title: Critical Infrastructure Protection: Elements of Risk
Author(s): Liz Jackson of the Critical Infrastructure Protection Program, George Mason University School of Law
Organization: George Mason University, School of Law's Critical Infrastructure Protection (CIP) Program
Publisher: George Mason University
Publishing Location: George Mason University
Edition: Unavailable
Pages: 111
Retrieved from: N/A
Hyperlink: http://www.steelcityre.com/documents/RiskMonograph_1207.pdf
Date of Publication: December 2007

Description:

- "The papers included in this monograph represent numerous perspectives on elements of risk and feature an array of authors working in the challenging field of homeland security. The papers address topics such as the definition of risk, assessment methodologies, and strategic approaches to risk management. Notably, the focus of this monograph is risk, and risk management, in the general sense. The monograph does not include papers delving into specific sectors, nor is it meant to endorse any one methodology or technology used in assessing and managing risk." [Introductory pages]

Additional Information:
The papers are:

- Security Risk Management: Implementing a National Framework for Success in the Post-9/11 World
  by Edward J. Jopeck and Kerry L. Thomas
- Intelligence Analysis for Strategic Risk Assessments
  by Geoffrey S. French
- The Meaning of Vulnerability in the Context of Critical Infrastructure Protection
  by William L. McGill and Bilal M. Ayyub
- Vulnerability Assessment of Arizona's Critical Infrastructure
  by Todd White, Samuel T. Ariaratnam, and Kraig Knutson
- Managing Risk in Critical Infrastructures Using Network Modeling
  by Thomas J. Mackin, Rudy Darken, and Ted G. Lewis
- Same Words, Different Meanings: The Need for Uniformity of Language and Lexicon in Security Analysis and Risk Management
  by Andrew G. Harter
- The Intangible Value of Security in a Volatile Global Economy
  by Robert P. Liscouski and Nir Kossovsky

3.3 Understanding CI Systems and Interdependencies

3.3.1 Modeling and Coordinating Interdependent Critical Infrastructures in Montréal

Title: Modeling and Coordinating Interdependent Critical Infrastructures in Montréal
Author(s): Benoit Robert, Luciano Morabito, and Irène Cloutier (Centre Risque & Performance, Department of Mathematics and Industrial Engineering, École Polytechnique de Montréal)
Organization: N/A
Publisher: George Mason School of Law
Publishing Location: United States of America
Edition: N/A
Pages: 3-6
Retrieved from: The Critical Infrastructure Protection (CIP) Report, Vol. 10, No. 11
Hyperlink:
http://cip.gmu.edu/archive/CIPHS_TheCIPReport_May2012_InternationalCriticalInfrastructure.pdf
Date of Publication: May 2012

Description:

- This article describes DOMINO, a modeling and mapping tool developed by the Centre Risque & Performance (CRP) of the École Polytechnique de Montréal.
- This tool allows "users to identify the interdependencies among the CI and anticipate the domino effects they can generate…DOMINO is a decision and planning assistance tool that makes it possible to respond to this set of problems." [p. 3]

3.3.2 Reducing Vulnerability of Critical Infrastructures - Methodological Manual

Title: Reducing Vulnerability of Critical Infrastructures - Methodological Manual
Author(s): Benoit Robert, Luciano Morabito (École Polytechnique de Montréal)
Organization: N/A
Publisher: Presses Internationales Polytechnique
Publishing Location: Canada
Edition: Unavailable
Pages: 57
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: 2011

Background:

- "This methodological manual describes an approach developed by the *Centre risque & performance* at the École Polytechnique de Montréal in partnership with the main LSNs [life support networks] on the Island of Montreal: electricity (Hydro-Québec), natural gas (GazMétro), telecommunications (Bell Canada), transportation (Quebec transport department), drinking water (city of Montreal), and civil security (city of Montreal - civil security centre). The approach has since been applied successfully in Quebec City as well." [p. 5]

Purpose:

- "The aim of this book is to establish a basic model to evaluate functional interdependencies among LSNs [life support networks] and implement tools to manage them. This will allow the competent authorities to anticipate domino effects among these infrastructures and thus avoid, or at least mitigate, their undesirable consequences. The book is structured as an operating manual, which makes it easy to apply this innovative approach." [p. 5]

Audience:

- "This manual is intended primarily for municipalities, government authorities, system managers and emergency measures officers who require tools to manage interdependencies among LSNs. It can also be used by those wishing to apply this methodology to evaluate interdependencies in different contexts, such as the management of a special event, the evaluation of interdependencies among departments within an organization or among the subsystems of a mechanical, electrical, information or other system, or even the evaluation of interdependencies among the actors in a project.
- The book can also be used by those who are interested in risk management and wish to understand the problems related to interdependencies among LSNs and the approach to evaluating such interdependencies proposed by the *Centre risque & performance*." [p. 5]

Description:

- This manual presents "the different steps of the methodology for evaluating functional and geographic interdependencies among LSNs. The objective of each step is briefly explained and the information that must be collected to complete it is presented in the form of an operating procedure. For each step, an example of the results obtained when the methodology was applied to the city of Montreal or Quebec is presented (the actual data from these examples has been modified to maintain confidentiality." [p. 21]
- In addition, this manual includes a section on information sharing, as it is one of the fundamental aspects of studying interdependencies.

3.3.3 A Method for Risk Modeling of Interdependencies in Critical Infrastructures

Title: A Method for Risk Modeling of Interdependencies in Critical Infrastructures
Author(s): I.B. Utne; P. Hokstad; J. Vatn
Organization: N/A
Publisher: Elsevier
Publishing Location: Unavailable
Edition: N/A
Pages: 671-678
Retrieved from: Reliability Engineering and System Safety, Vol. 96, No. 6
Hyperlink: N/A
Date of Publication: June 2011

Abstract:
"Failures in critical infrastructures may be hazardous to population, economy, and national security. There can be strong interdependencies between various infrastructures, but these interdependencies are seldom accounted for in current risk and vulnerability analyses. To reduce probability and mitigate consequences of infrastructure failures, these interdependencies have to be assessed. The objective of this paper is to present a method for assessing interdependencies of critical infrastructures, as part of a cross-sector risk and vulnerability analysis. The method is based on a relatively simple approach applicable for practitioners, but may be extended for more detailed analyses by specialists. Examples from a case study with the Emergency Preparedness Group of the city of Oslo, Norway, are included." [p. 671]

Key words: Critical infrastructures; Risk analyses; Interdependencies; Safety

3.3.4 Interdependencies Modelling Project Software Development Final Report

Title: Interdependencies Modelling Project Software Development Final Report
Author(s): Bruce Nelson (Coordinator, Ontario Critical Infrastructure Assurance Program), Philip O'Neill (President, Quantitative Decision Support, Inc.)
Organization: Emergency Management Ontario, Public Safety Canada
Publisher: Emergency Management Ontario
Publishing Location: Unavailable
Edition: N/A
Pages: 28
Retrieved from: Unavailable
Hyperlink: Unavailable
Date of Publication: March 31, 2010

Background:

- "The Critical Infrastructure Interdependencies Modelling Project is a joint venture between the Government of Canada and the Province of Ontario. The respective lead agencies are Public Safety Canada and Emergency Management Ontario.
- The Modelling Project has been a five year project to develop a critical infrastructure (CI) dependencies and interdependencies modelling tool. The result of the project is a baseline risk model of Ontario's CI sectors.
- To fulfill the requirements of the Ontario Critical Infrastructure Assurance Program (OCIAP), this project adapted a Y2K, one time event, CI risk modelling tool into a dynamic modelling tool. The project commenced in January, 2005 and concluded March 31, 2010." [p. 1]

Description:

- This report describes the Critical Infrastructure Interdependencies Modelling Project, with a focus on risk evaluation for complex and interconnected infrastructures.

3.3.5 An Approach to Identifying Geographic Interdependencies among Critical Infrastructures

Title: An Approach to Identifying Geographic Interdependencies among Critical Infrastructures
Author(s): Benoit Robert, Luciano Morabito
Organization: N/A
Publisher: Inderscience Publishers
Publishing Location: Unavailable
Edition: N/A
Pages: 17-30
Retrieved from: International Journal of Critical Infrastructures, Vol. 6, No. 1
Hyperlink: N/A
Date of Publication: 2010

Abstract:
Interdependencies among Critical Infrastructures (CIs) are the basis for domino effects that may have serious consequences for society. Especially in urban areas, the high density of these infrastructures and their geographic proximity may result in failures due to geographic interdependencies, one of the four types of interdependencies that exist among CIs. Studying the issue of geographic interdependencies raises a specific problem that must be addressed. Such a study necessarily requires information on the location of system infrastructures in order to determine their proximity. Access to this kind of information is one of the major difficulties associated with the study of geographic interdependencies. Because this kind of information is confidential, systems are not willing to share it. This article presents an approach that makes it possible to study geographic interdependencies among CIs but requires only a minimum of information on the specific location of system infrastructures. Based on the concept of so-called flexible cartography, this approach provides relevant results for the processing of interdependencies, while respecting organisations' confidentiality constraints.

Keywords: critical infrastructures; geographic interdependencies; confidentiality; protective measures; preventive measures; warning mechanisms; domino effect; system infrastructures; flexible cartography.

3.3.6 Managing Critical Infrastructure Interdependencies: The Ontario Approach

Title: Managing Critical Infrastructure Interdependencies: The Ontario Approach
Author(s): Bruce D. Nelson
Organization: Emergency Management Ontario, Ministry of Community Safety and Correctional Services
Publisher: John Wiley & Sons, Inc.
Publishing Location: Unavailable
Edition: N/A
Pages: 1-10
Retrieved from: Wiley Handbook of Science and Technology for Homeland Security, from the Wiley Online Library website
Hyperlink: http://onlinelibrary.wiley.com/doi/10.1002/9780470087923.hhs243/pdf
Date of Publication: 2009

Abstract:
"The Province of Ontario developed the Critical Infrastructure Assurance Program based upon risk management, business continuity process, and the collaboration of three levels of government and the private sector. It addresses the resiliency of systems and networks and their ability to function at some level throughout a threat. It is an all-hazards approach that concentrates its efforts in the prevention and mitigation pillars of emergency management. The systems are addressed by sectors and their information sharing networks are an integral part of the program. The program includes a modeling program that is fed by the work of the sectors and addresses the strength of relationships amongst the sectors' dependencies and interdependencies. The program's work is validated through an annual interdependency exercise involving all sectors and smaller exercises on particular threats or identified vulnerabilities between sectors. The most valuable part of the program is the sharing of knowledge throughout the information-sharing network." [p. 1]

Keywords: all-hazards; resiliency; systems; risk management; business continuity process; collaboration

3.3.7 Cyber and Physical Infrastructure Interdependencies

Title: Cyber and Physical Infrastructure Interdependencies
Author(s): Andjelka Kelic, Drake E. Warren, Laurence R. Phillips
Organization: Sandia National Laboratories
Publisher: Unavailable
Publishing Location: United States of America
Edition: Unavailable
Pages: 66
Retrieved from: N/A
Hyperlink: http://prod.sandia.gov/techlib/access-control.cgi/2008/086192.pdf
Date of Publication: September 2008

Abstract:
"The goal of the work discussed in this document is to understand the risk to the nation of cyber attacks on critical infrastructures. The large body of research results on cyber attacks against physical infrastructure vulnerabilities has not resulted in clear understanding of the cascading effects a cyber-caused disruption can have on critical national infrastructures and the ability of these affected infrastructures to deliver services. This document discusses current research and methodologies aimed at assessing the translation of a cyber-based effect into a physical disruption of infrastructure and thence into quantification of the economic consequences of the resultant disruption and damage. The document discusses the deficiencies of the existing methods in correlating cyber attacks with physical consequences. The document then outlines a research plan to correct those deficiencies. When completed, the research plan will result in a fully supported methodology to quantify the economic consequences of events that begin with cyber effects, cascade into other physical infrastructure impacts, and result in degradation of the critical infrastructure's ability to deliver services and products.

This methodology enables quantification of the risks to national critical infrastructure of cyber threats. The work addresses the electric power sector as an example of how the methodology can be applied. "[p. 3]

3.3.8 Modelling Interdependencies Among Critical Infrastructures

Title: Modelling Interdependencies Among Critical Infrastructures
Author(s): Benoit Robert, Renaud De Calan, Luciano Morabito (École Polytechnique de Montréal)
Organization: Unavailable
Publisher: Inderscience Enterprises Ltd.
Publishing Location: Switzerland
Edition: N/A
Pages: 392-408
Retrieved from: International Journal of Critical Infrastructures, Vol. 4, No.4
Hyperlink: N/A
Date of Publication: 2008

Abstract:
"Over the years, critical infrastructures (CIs) have become increasingly automated and interlinked. This linkage between CIs results in a very complex and dynamic system which increases their vulnerability to failures. In fact, interdependencies between CIs are a true means of propagation of hazards from one network to another. Thus, when an infrastructure is experiencing difficulties and failures, it can rapidly generate a cascading effect affecting the other infrastructures. Identifying, understanding and modelling these interdependencies is thus necessary to prevent these cascading effects. This paper presents a model developed to understand the interdependencies between CIs and to prevent cascading effects from happening. Based on the resources exchanged by CIs, this model allows the visualisation and the anticipation of domino effects in time and space, allowing CI managers to set up convenient preventive and protective measures in order to avoid their propagation." [p. 392]

3.3.9 The Operational Tools for Managing Physical Interdependencies Among Critical Infrastructures

Title: The Operational Tools for Managing Physical Interdependencies Among Critical Infrastructures
Author(s): Benoit Robert, Luciano Morabito (École Polytechnique de Montréal)
Organization: N/A
Publisher: Inderscience Enterprises Ltd.
Publishing Location: Switzerland
Edition: N/A
Pages: 353-367
Retrieved from: International Journal of Critical Infrastructures, Vol. 4, no. 4
Hyperlink: N/A
Date of Publication: 2008

Abstract:
"As a result of advances in information technology and the necessity of improved efficiency, critical infrastructures (CIs) have become increasingly automated and interlinked over the years. This linkage between CI results in a very complex and dynamic system. However, this growing complexity of CI and their interdependencies reveals new vulnerabilities. In fact, the interdependencies between CI are a true means of the propagation of hazards from one network to another. Understanding these interdependencies is necessary to prevent any cascading effects to affect the functioning of these infrastructures. This paper presents a concrete set of tools enabling the management of physical interdependencies among the CI. Based on the resources exchanged by CI, these tools (consequence curves and flexible cartographic representations) allow the visualisation of the evolution of domino effects in time and space, giving the CI managers the potential to set up convenient preventive and protective measures in order to avoid their propagation." [p. 353]

3.3.10 Visualizing Cascading Failures in Critical Cyber Infrastructure

Title: Visualizing Cascading Failures in Critical Cyber Infrastructure
Author(s): Jason K. Kopylec, Anita D. D'Amico and John R. Goodall
Organization: N/A
Publisher: Springer US
Publishing Location: Unavailable
Edition: Unavailable
Pages: 351-364
Retrieved from: Chapter 25 in *Critical Infrastructure Protection*
Hyperlink: http://www.springerlink.com/content/u1685022806012m5/fulltext.pdf
Date of Publication: 2008

Abstract
"This article explores the relationship between physical and cyber critical infrastructures, focusing on how threats and disruptions in the physical infrastructures can cascade into failures within cyber infrastructure. Through interviews with critical infrastructure protection experts and practitioners, we examined the issues in dealing with cyber infrastructure, including challenges with the management and organization of massive amounts of data that is geographically and logically disparate. Based on that understanding, we designed a system, named Cascade, for visualizing the cascading effects of physical infrastructure failures into the cyber infrastructure. Cascade will provide situational awareness to people who plan for and respond to crises related to Information and Communication Technology. Cascade shows how threats to physical infrastructures such as power, transportation, and communications can affect the networked enterprises that comprise the cyber infrastructure. Our approach applies the concept of punctualization from Actor-Network Theory to expose only the relevant disruptive effects and as an organizing principle for large collections of disparate infrastructure data. In particular, we show how to expose the critical relationships between the physical and cyber infrastructures. We discuss the availability of infrastructure data, and how this information can be depicted visually to maximize comprehension. This article also addresses the issue of representing both the logical and geospatial relationships within the cyber infrastructure. The resulting system design provides access to the cyber infrastructure's dependencies on other critical infrastructures, for use during disaster planning or crisis response." [p. 351]

3.3.11 The Preventive Approach to Risks Related to Interdependent Infrastructures

Title: The Preventive Approach to Risks Related to Interdependent Infrastructures
Author(s): Robert, Luciano Morabito and Olivier Quenneville (École Polytechnique de Montréal)
Organization: N/A
Publisher: Inderscience Enterprises Limited
Publishing Location: Switzerland
Edition: N/A
Pages: 166-182
Retrieved from: International Journal of Emergency Management, Vol. 4, Issue 2
Hyperlink: N/A
Date of Publication: 2007

Abstract:
"Life Support Networks (LSNs) assure that society functions correctly through provision of essential resources such as telecommunications and energy--in other words, the correct functioning of society is guaranteed through the correct functioning of LSNs. New vulnerabilities have been revealed through the growing complexity of both LSNs and their interdependencies. Between-network hazards can truly be propagated through these interdependencies. Current risk management methods (often based on aiming at interdependency modeling, worst case scenario analysis, and/or probabilistic approaches) are hardly applicable to LSN and other complex and dynamic systems' concrete realities. Jointly with multiple partners, the risk and performance center has developed a new proactive risk management methods based on harmful LSN consequence prevention and anticipation to compensate for these gaps." [p. 166]

3.3.12 Identification of Sources of Failures and their Propagation in Critical Infrastructures from 12 Years of Public Failure Reports

Title: Identification of Sources of Failures and their Propagation in Critical Infrastructures from 12 Years of Public Failure Reports
Author(s): Hafiz Abdur Rahman, Konstantin Beznosov, José R. Martí (Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada)
Organization: Infrastructures Interdependencies Simulation (I2SIM) Team, University of British Columbia
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 12
Retrieved from: Document # jiirp i2sim 017, Conference paper, CRIS, Third International Conference on Critical Infrastructures, Alexandria, VA, September 2006
Hyperlink: http://www.ece.ubc.ca/~jiirp/JIIRP_Open_Publications/jiirp_i2c_017.pdf
Date of Publication: September 2006

Description:
"In this work, we have identified interdependencies between CITI [Communication and Information Technology Infrastructure] and other infrastructures based on some key factors, such as, origin of failures, impact of failures in spatial and temporal dimensions, effect of failure on public safety and their propagation from CITI to other critical infrastructures and vice versa. More specifically, we would like to answer questions such as, what are the main causes of infrastructure failures, what is the nature of their impact; what locality is affected by them and their geographical locations, how their fatality changed over time, and how infrastructures are related to each other. In the absence of any formal model of interdependencies between CITI and other critical infrastructures, our findings should give useful ideas to the policy makers, practitioners and researchers. In Related Work section, we discuss previous works to classify and interpret infrastructure related failures. In Approach and Methods section, we give a brief overview of our own methodology. In Failure Database section, we give a brief description of our failure database. In Results section, we summarize the results of our analysis. Finally, in Conclusions section, we discuss the contributions of this research and future research directions." [p. 1-2]

3.3.13 A Human-Centered Conceptual Model of Disasters Affecting Critical Infrastructures

Title: A Human-Centered Conceptual Model of Disasters Affecting Critical Infrastructures
Author(s): Philippe Kruchten, Carson Woo, Mandana Sotoodeh, Kafui Monu
Organization: Infrastructures Interdependencies Simulation (I2SIM) Team, University of British Columbia
Publisher: University of British Columbia
Publishing Location: Vancouver, British Columbia
Edition: N/A
Pages: 28 (slides)
Retrieved from: Document # jiirp i2sim 009: Presentation, Joint Infrastructure Interdependencies Research Program (JIIRP) Industry Symposium
Hyperlink: http://www.ece.ubc.ca/~jiirp/JIIRP_Open_Publications/jiirp_i2c_009.pdf
Date of Publication: February 24th, 2006

Description:

- This presentation provides an overview of a metamodel, which takes a human-centered approach to disasters and attempts to understand how they affect people through critical infrastructure.

The focus of this project is:

- "Impact of disaster on human population
  - not just dollar value
- Interdependencies between infrastructure
- Physical interdependencies
  - Failure in A leads to failure in B
- Communication and coordination
  - “human in the loop” someone in X speaks to someone in Y" [slide 5]

Additional Information:
This model is based on four groups of concepts. They are:

1. "Regions and people, wellness
2. Infrastructures: electrical, transport, etc.
3. Events: disaster trigger, initiatives
4. Communication and coordination" [slide 6]

3.3.14 Infrastructure Simulations of Disaster Scenarios

Title: Infrastructure Simulations of Disaster Scenarios
Author(s): Gerard P. O'Reilly, David J. Houck, Eunyoung Kim, Thomas B. Morawaski, David D. Picklesimer, Huseyin Uzunalioglu (Bell Labs, Lucent Technologies, U.S.A)
Organization: N/A
Publisher: VDE Verlag GMBH
Publishing Location: Germany
Edition: N/A
Pages: 205-210
Retrieved from: Conference Publications, 11th International Telecommunications Network Strategy and Planning Symposium
Hyperlink: N/A
Date of Publication: 2004

Abstract:
"Critical national infrastructures for transportation, power, finance, and other basic industries rely heavily on information and telecommunications networks (voice, data, Internet) to provide services and conduct business. While these networks tend to be highly reliable, disasters may lead to extended outages requiring days/weeks to repair. These outages cause loss of business continuity, and financial transaction failures. This paper describes a simulation model of communications network disasters, their network performance, and their impact on other critical infrastructures using shipping through a port as an example." [p. 205]

3.3.15 Infrastructure Interdependencies: Concepts and Importance in Security Vulnerability Assessments

Title: Infrastructure Interdependencies: Concepts and Importance in Security Vulnerability Assessments
Author(s): Jim Peerenboom and Ron Fisher
Organization: Argonne National Laboratory, Sponsored by Information Analysis and Infrastructure Protection Directorate, U.S. Department of Homeland Security
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: 26
Retrieved from: Slideshow for the API Security Vulnerability Assessment Workshop, April 23, 2003, Houston, Texas
Hyperlink: N/A
Date of Publication: 2003

Description:
This presentation provides an overview of some of the key issues that stem from infrastructure interdependencies. It discusses:

- Concepts and issues which arise from interdependencies;
- Types of infrastructure interdependencies;
- Examples of interdependencies;
- Approach that is needed to analyze infrastructure interdependencies;
- Types of interdependence failures;
- Challenges for security and reliability;
- Vulnerabilities resulting from infrastructure interdependencies; and
- Lessons learned.

3.3.16 Studying the Chain Reaction: Interdependency Studies Show How the Dominoes Can Fall and What Infrastructure Operators Must Do to Keep Them Standing

Title: Studying the Chain Reaction: Interdependency Studies Show How the Dominoes Can Fall and What Infrastructure Operators Must Do to Keep Them Standing
Author(s): James P. Peerenboom, Ronald E. Fisher, Steven M. Rinaldi, and Terrance K. Kelly
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 10
Retrieved from: Electric Perspectives, Edison Electric Institute, January/February 2002
Hyperlink: N/A
Date of Publication: 2002

Description:

- This paper begins by describing several examples of disruptions to interconnected infrastructure.
- Then, the meaning of interdependency is explored, including a discussion of gaps that exist in understanding and analyzing interdependent infrastructures.
- Next, the paper attempts to 'fit the pieces together' in order to understand failures in interdependent infrastructures.
- Lastly, other dimensions of the infrastructure environment (such as the operating state of each infrastructure or economic business concerns) are considered.

3.3.17 Infrastructure Interdependencies Tabletop Exercise

Title: Infrastructure Interdependencies Tabletop Exercise
Author(s): Infrastructure Protection Subcommittee of the Utah Olympic Public Safety Command
Organization: Infrastructure Protection Subcommittee of the Utah Olympic Public Safety Command
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: 65 (slides)
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: November 28, 2000

Purpose of the Exercise:

- "Help ensure the reliability and security of critical infrastructures - before, during, and after the 2002 Winter Olympic Games
- "Provide a foundation for addressing critical infrastructure protection needs within the State of Utah " [Slide 7]

Description of the Exercise:

- "Black Ice requires a situational assessment based on the scenario provided
- Participants (players) need to think broadly about the interdependencies within and among the critical infrastructures, and their importance in terms of responding to and recovering from the infrastructure disruptions identified in the scenario" [Slide 12]

Description of the Document:

- This presentation provides an outline of the Black Ice exercise, including the timeline, rules of engagement, player participation, scenarios, impacts on infrastructure, discussion questions, and supplementary information.

3.3.18 Workshop on Future Directions in Critical Infrastructure Modeling and Simulation

Title: Workshop on Future Directions in Critical Infrastructure Modeling and Simulation
Author(s): Dr. Nabil Adam (Chair), Infrastructure & Geophysical Division, DHS Science and Technology Directorate
Organization: Department of Homeland Security
Publisher: Department of Homeland Security
Publishing Location: Unavailable
Edition: Final Report
Pages: 254
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: December 23, 2008

Background:

- "From October 28 through 30, 2008, the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) hosted a workshop, "Future Directions in Critical Infrastructure Modeling and Simulation," on the use of modeling and simulation (M&S) to effectively deal with the consequences of catastrophic events on critical infrastructure." [p. vii]

Purpose:

- "The purpose of the workshop was to help S&T formulate sound investment decisions, both near- and long-term, as well as research strategy, plans, and objectives for M&S of the Nation's critical infrastructure and key resources (CIKR)." [p. vii]

Description:
"This report summarizes the workshop's recommendations. They are arranged in five areas:

A. Resources for critical infrastructure modeling and simulation...
B. Data issues...
C. Human and organizational factors in the use and management of DHS modeling and simulation...
D. Model development...
E. Verification and validation." [p. vii-viii]

Additional Information:
This report is structured as follows:

- "Section II, The User Perspective, discusses how current M&S users see the challenges and opportunities of modeling and simulation for helping protect critical infrastructure.
- Section III, State-of-the-Art Simulations, Models, Tools, and Methods, summarizes the state of the art of M&S for representing and analyzing critical infrastructure.
- Section IV, Recommendations, summarizes the workshop's recommendations, as well as the report writers' personal recommendations.
- Section V, Acronyms and Abbreviations, spells out acronyms and abbreviations used in this report.
- Finally, an appendix presents the main presentation, the panel discussions, the working group sessions reports, and the synthesis group "out brief"." [p. 3]

3.3.19 The State of the Art in Critical Infrastructure Protection: A Framework for Convergence

Title: The State of the Art in Critical Infrastructure Protection: A Framework for Convergence
Author(s): Ali A. Ghorbani, Ebrahim Bagheri (Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada)
Organization: N/A
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: 215-244
Retrieved from: International Journal of Critical Infrastructures, Vol. 4, No. 3
Hyperlink: N/A
Date of Publication: 2008

Abstract:
"The protection of critical infrastructure systems has recently become a major concern for many countries. This is due to the effect of these systems on the daily lives of all citizens and the high possibility of disruption because of their complex structure and hidden interdependencies, which subsequently attract the attention of many researchers and scientists. The investigations of researchers have encompassed issues of national security, policymaking, infrastructure system organisation, and behaviour analysis and modelling. In this paper, we look into the latter subject and explore the attempts that have been made. Based on the available schemes and the requirements of this area, we propose a five-dimensional framework that introduces the major research necessities in this field. Among the various available schemes, we study ten of the most recently developed and/or influential systems. A comparison of these schemes based on the features of our proposed framework is made. The comparison allows us to conclude our examination with the identification of current research strengths and guidelines for future work." [p. 215]

Keywords: critical infrastructures; infrastructure protection; modelling; simulation.

Description:
- This paper contributes to the body of research that attempts to understand the dynamic behavior of infrastructure systems.

Additional Information:
This paper is structured as follows:
- Section 1: Introduction
- Section 2: Description of ten critical infrastructure modeling or analysis schemes
- Section 3: Introduction of the proposed framework
- Section 4: Comparison of the schemes introduced in Section 2
- Section 5: Discussions and future work
- Section 6: Conclusion

3.3.20 Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research

Title: Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research
Author(s): P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann
Organization: Idaho National Laboratory (a U.S. Department of Energy National Laboratory)
Publisher: Idaho National Laboratory
Publishing Location: Idaho Falls, Idaho
Edition: Unavailable
Pages: 126
Retrieved from: N/A
Hyperlink: http://cipbook.infracritical.com/book3/chapter2/ch2ref2a.pdf
Date of Publication: August 2006

Abstract:
"The Nation's health, wealth, and security rely on the production and distribution of certain goods and services. The array of physical assets, processes, and organizations across which these goods and services move are called critical infrastructures." This statement is as true in the U.S. as in any country in the world. Recent world events such as the 9-11 terrorist attacks, London bombings, and gulf coast hurricanes have highlighted the importance of stable electric, gas and oil, water, transportation, banking and finance, and control and communication infrastructure systems.

Be it through direct connectivity, policies and procedures, or geospatial proximity, most critical infrastructure systems interact. These interactions often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries. The modeling and analysis of interdependencies between critical infrastructure elements is a relatively new and very important field of study.

The U.S. Technical Support Working Group (TSWG) has sponsored this survey to identify and describe this current area of research including the current activities in this field being conducted both in the U.S. and internationally. The main objective of this study is to develop a single source reference of critical infrastructure interdependency modeling tools (CIIMT) that could be applied to allow users to objectively assess the capabilities of CIIMT. This information will provide guidance for directing research and development to address the gaps in development. The results will inform researchers of the TSWG Infrastructure Protection Subgroup of research and development efforts and allow a more focused approach to addressing the needs of CIIMT end-user needs.

This report first presents the field of infrastructure interdependency analysis, describes the survey methodology, and presents the leading research efforts in both a cumulative table and through individual datasheets. Data was collected from open source material and when possible through direct contact with the individuals leading the research." [p. iii]

3.4 Protecting CI

3.4.1 The CIP Report

Title: The CIP Report
Author(s): N/A
Organization: George Mason University
Publisher: Center for Infrastructure Protection and Homeland Security, George Mason University
Publishing Location: Unavailable
Edition: N/A
Pages: N/A
Retrieved from: Center for Infrastructure Protection and Homeland Security website
Hyperlink: http://cip.gmu.edu/publications/books
Date of Publication: Monthly publications since July 2002

Overview:
"*The CIP Report* is a monthly, electronic newsletter for professionals in industry, government, and academia who have an interest in critical infrastructure protection (CIP). The newsletter provides the latest information about CIP including emerging legislation, government initiatives and leaders, and academic endeavors. All versions of *The CIP Report* are available in *The CIP Report* Archive with a complete listing of all volumes of *The CIP Report* organized by date and topic"[7].

Additional Information:
The following issues were released between January and September of 2012. A complete collection of the monthly issues published since July of 2002 is available in *The CIP Report* Archive.

- September 2012: Water
- August 2012: Smart Grid
- July 2012: Surface Transportation
- June 2012: CIP/HS Update
- May 2012: International CIP
- April 2012: Cybersecurity
- March 2012: Commercial Facilities
- February 2012: Commercial Facilities
- January 2012: Alternative Energy

[7] From http://cip.gmu.edu/the-cip-report

3.4.2 Regional Resiliency Assessment Program Fact Sheet

Title: Regional Resiliency Assessment Program Fact Sheet
Author(s): Office of Infrastructure Protection, Protective Security Coordination Division
Organization: Department of Homeland Security
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 2
Retrieved from: Tampa Bay Regional Planning Council website
Hyperlink:
http://www.tbrpc.org/council_members/council_presentations/2011/021411/Gagnon_DHS_RRAP_02142011.pdf
Date of Publication: October 2010

Description:

- This factsheet provides a quick overview of the Office of Infrastructure Protection's Regional Resiliency Assessment Program (RRAP) and its methodology.

Additional Information:

- "The Regional Resiliency Assessment Program (RRAP) is a cooperative, Office of Infrastructure Protection (IP) led interagency assessment of specific critical infrastructure and regional analysis of the surrounding infrastructure." [p. 1]
- "The RRAP methodology employs an enhanced assessment methodology that identifies critical infrastructure dependencies, interdependencies, cascading effects, resiliency characteristics, and regional capability and security gaps. The resulting analysis details the risk and consequences of an incident or attack, and the integrated preparedness and protection capabilities of the critical infrastructure owners and operators, local law enforcement, and emergency response organizations. The results are used to enhance the overall security posture of the facilities, the surrounding communities, and the geographic region using risk-based investments in equipment, planning, training, processes, procedures, and resources." [p. 1]

3.4.3 Defending Critical Infrastructure

Title: Defending Critical Infrastructure
Author(s): Gerald Brown, Matthew Carlyle, Javier Salmerón, Kevin Wood
Organization: Operations Research Department, Naval Postgraduate School, Monterey, California
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 530-544
Retrieved from: Interfaces, Vol. 36, No. 6
Hyperlink: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA486996
Date of Publication: November-December 2006

Abstract:
"We apply new bilevel and trilevel optimization models to make critical infrastructure more resilient against terrorist attacks. Each model features an intelligent attacker (terrorists) and a defender (us), information transparency, and sequential actions by attacker and defender. We illustrate with examples of the US Strategic Petroleum Reserve, the US Border Patrol at Yuma, Arizona, and an electrical transmission system. We conclude by reporting insights gained from the modeling experience and many "red-team" exercises. Each exercise gathers open-source data on a real-world infrastructure system, develops an appropriate bilevel or trilevel model, and uses these to identify vulnerabilities in the system or to plan an optimal defense." [p. 530]

Key words: critical infrastructure protection; bilevel program; trilevel program; mixed-integer program; homeland security; homeland defense.

3.4.4 Critical Infrastructure Protection in Homeland Security - Defending a Networked Nation

Title: Critical Infrastructure Protection in Homeland Security - Defending a Networked Nation
Author(s): Ted G. Lewis (Naval Postgraduate School, Monterey, California)
Organization: N/A
Publisher: John Wiley & Sons, Inc.
Publishing Location: Hoboken, New Jersey and Canada
Edition: N/A
Pages: 483
Retrieved from: N/A
Hyperlink: http://ebookbrowse.com/critical-infrastructure-protection-in-homeland-security-defending-a-networked-nation-lewis-wiley-2006-pdf-d342540897
Date of Publication: 2006

Description:

- "A scientific approach to the new field of critical infrastructure protection
- This book offers a unique scientific approach to the new field of critical infrastructure protection: it uses network theory, optimization theory, and simulation software to analyze and understand how infrastructure sectors evolve, where they are vulnerable, and how they can best be protected. The author demonstrates that infrastructure sectors as diverse as water, power, energy, telecommunications, and the Internet have remarkably similar structures. This observation leads to a rigorous approach to vulnerability analysis in all of these sectors. The analyst can then decide the best way to allocate limited funds to minimize risk, regardless of industry sector.
- The key question addressed in this timely book is: What should be protected and how? The author proposes that the answer lies in allocating a nation's scarce resources to the most critical components of each infra-structure--the so-called critical nodes. Using network theory as a foundation, readers learn how to identify a small handful of critical nodes and then allocate resources to reduce or eliminate risk across the entire sector.
- A comprehensive set of electronic media is provided on a CD-ROM in the back of the book that supports in-class and self-tutored instruction. Students can copy these professionally produced audio-video lectures onto a PC (Microsoft Windows(r) and Apple Macintosh(r) compatible) for repeated viewing at their own pace. Another unique feature of the book is the open-source software for demonstrating concepts and streamlining the math needed for vulnerability analysis. Updates, as well as a discussion forum, are available from www.CHDS.us.
- This book is essential for all corporate, government agency, and military professionals tasked with assessing vulnerability and developing and implementing protection systems. In addition, the book is recommended for upper-level undergraduate and graduate students studying national security, computing, and other disciplines where infrastructure security is an issue"[8].

[8] From http://ca.wiley.com/WileyCDA/WileyTitle/productCd-0471786284.html

3.4.5 Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art

Title: Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art
Author(s): Jose M. Yusta, Gabriel J. Correa, Roberto Lacal-Arántegui
Organization: N/A
Publisher: Elsevier
Publishing Location: Unavailable
Edition: N/A
Pages: 6100-6119
Retrieved from: Energy Policy, Vol. 39, No. 10
Hyperlink: N/A
Date of Publication: October 2011

Abstract:
"This work provides an update of the state-of-the-art on energy security relating to critical infrastructure protection. For this purpose, this survey is based upon the conceptual view of OECD countries, and specifically in accordance with EU Directive 114/08/EC on the identification and designation of European critical infrastructures, and on the 2009 US National Infrastructure Protection Plan.
The review discusses the different definitions of energy security, critical infrastructure and key resources, and shows some of the experiences in countries considered as international reference on the subject, including some information-sharing issues. In addition, the paper carries out a complete review of current methodologies, software applications and modelling techniques around critical infrastructure protection in accordance with their functionality in a risk management framework.
The study of threats and vulnerabilities in critical infrastructure systems shows two important trends in methodologies and modelling. A first trend relates to the identification of methods, techniques, tools and diagrams to describe the current state of infrastructure. The other trend accomplishes a dynamic behaviour of the infrastructure systems by means of simulation techniques including systems dynamics, Monte Carlo simulation, multi-agent systems, etc." [p. 6100]

3.4.6 CRN Report - Focal Report 4 - Critical Infrastructure Protection: Protection Goals

Title: CRN Report - Focal Report 4 - Critical Infrastructure Protection: Protection Goals
Author(s): Elgin Brunner, Myriam Dunn Cavelty, Jennifer Giroux, Manuel Suter
Organization: Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH (Swiss Federal Institute of Technology) Zurich
Publisher: Center for Security Studies (CSS), ETH Zürich
Publishing Location: Zürich, Switzerland
Edition: N/A
Pages: 27
Retrieved from: Center for Security Studies website
Hyperlink: http://www.css.ethz.ch/publications/pdfs/Focal-Report-4-CIP.pdf
Date of Publication: February 2010

Description:
Structure and Content of Focal Report

- "This report will explore the manner in which protection goals are defined in CIP [critical infrastructure protection]. In doing so, we will identify and analyze the protection goals in various countries and address the following questions based on the empirical analysis:
  - What protection goals do states define in the practice of CIP?
  - What purpose do they serve?
  - What aspects do they cover?
  - Who defines them?
- In conclusion, we will discuss what seems to be missing from the CIP discussion: how applicable and useful are protection goals for CIP and what aspects they should cover.

Additional Information:
The report has three parts:

- The first part examines how protection goals are handled in eight countries: Australia; Canada; Germany; Netherlands; Norway; Sweden; the United Kingdom; and the United States.
- The second part strives to evaluate these practices with regards to the above questions and compare them to the PLANAT model.
- The third part is the annex, containing a) excerpts sketching the protection goals in the policy documents analyzed and b) an annotated bibliography." [p. 4]

3.5 Recovering from Disruptions to CI

3.5.1 Dynamic Recovery of Critical Infrastructures: Real-Time Temporal Coordination

Title: Dynamic Recovery of Critical Infrastructures: Real-Time Temporal Coordination
Author(s): José R. Martí, Jorge A. Hollman, Carlos Ventura and Juri Jatskevicch (University of British Columbia)
Organization: N/A
Publisher: Inderscience Publishers
Publishing Location: Unavailable
Edition: N/A
Pages: 17-31
Retrieved from: International Journal of Critical Infrastructures, Vol. 4, Nos. 1/2
Hyperlink: http://www.i2sim.ca/
Date of Publication: 2008

Abstract:
"This paper takes a systems engineering approach to the problem of operations coordination among multiple infrastructures to minimise the impact of large disasters on human lives. Temporal coordination is essential to avoid bottlenecks in the simultaneous recovery of multiple infrastructures systems. A solution framework is presented in terms of multiple-delay difference equations which bring out the temporal interdependencies among infrastructures. The present work is part of an effort by the Government of Canada, through the Natural Sciences and Engineering Research Council (NSERC) and Public Safety and Emergency Preparedness Canada (PSEPC) to fund research to develop innovative ways to mitigate large disaster situations." [p. 17]

3.5.2 Dynamic Islanding of Critical Infrastructures, A Suitable Strategy to Survive and Mitigate Critical Events

Title: Dynamic Islanding of Critical Infrastructures, A Suitable Strategy to Survive and Mitigate Critical Events
Author(s): J.A. Hollman, J.R. Marti, J. Jatskevich, K.D. Srivastava
Organization: Infrastructures Interdependencies Simulation (I2SIM) Team, University of British Columbia
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 11
Retrieved from: Document # jiirp i2sim 012 - Conference paper, CNIP, Rome March 28-29, 2006
Hyperlink: http://www.ece.ubc.ca/~jiirp/JIIRP_Open_Publications/jiirp_i2c_012.pdf
Date of Publication: March 2006

Abstract
"This paper presents specific guidelines for policy makers with the objective to develop and enhance cooperation among critical infrastructures operators. The proposed actions are an effective means to increase the resiliency of the National Critical Infrastructures (NCIs) based on a dynamic islanding scheme which depends on the considered emergency scenario. The present work emerges in response to the Public Safety and Emergency Preparedness of Canada (PSEPC) Modernization of the Emergency Preparedness Act consultation process [1] and is part of the Joint Infrastructure Interdependencies Research Project (JIIRP), sponsored by PSEPC." [p. 1]

Keywords: National Critical Infrastructures, Islanding, Survival, Dynamic Segmentation

3.5.3 Recovering from Disruptions of Interdependent Critical Infrastructures

Title: Recovering from Disruptions of Interdependent Critical Infrastructures
Author(s): James Peerenboom, Ronald Fisher, and Ronald Whitfield
Organization: Infrastructure Assurance Center, Argonne National Laboratory
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 12
Retrieved from: Prepared for CRIS/DRM/IIT/NSF Workshop on "Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures", Lyceum, Alexandria, Virginia, September 10-11, 2001
Hyperlink: Unavailable
Date of Publication: 2001

Abstract:
"The security, economic prosperity, and social well being of the nation depend on the reliable functioning of our increasingly complex and interdependent infrastructures – and on our ability to rapidly restore service when they are disrupted or degraded. Infrastructures include energy systems (electric power, oil, natural gas), water supply systems, telecommunications, transportation, banking and finance, and emergency and government services. In the new economy, these interconnected infrastructures have become increasingly fragile and subject to disruptions that can have broad regional, national, and global consequences. Understanding such consequences requires understanding infrastructure vulnerabilities, mitigation techniques, and service restoration strategies. Because the time needed to return a damaged component of one infrastructure to service can depend on the states of other infrastructures, there are large uncertainties about the amount of time needed for restoring an infrastructure to service. This paper discusses four general categories of infrastructure interdependencies (physical, cyber, geographic, and logical), highlights recent real-life examples of cascading disruptions that have affected multiple infrastructures, and provides an overview of the analytic approaches being used by Argonne National Laboratory to estimate the amount of time needed for activities that must be completed to restore a given infrastructure component, such as a natural gas compressor station or electric substation, a specific infrastructure system, or an interdependent set of infrastructures, to an operational state. Examples of repair sequences for disrupted infrastructures are provided and results from CI3 (Critical Infrastructures Interdependencies Integrator), a Monte Carlo simulation tool, are presented to illustrate risk management concepts and issues. The impact of backup systems or other mitigation mechanisms that reduce interdependence and restoration problems are also described." [p. 1]

3.6 Clarifying Roles and Improving Collaboration

3.6.1 Roles and Responsibilities

3.6.1.1 Who Does What? Critical Infrastructure Protection in the Canadian Government

Title: Who Does What? Critical Infrastructure Protection in the Canadian Government
Author(s): John B. Hay
Organization: Canadian Centre of Intelligence and Security Studies (CCISS), the Norman Paterson School of International Affairs
Publisher: Carleton University
Publishing Location: Ottawa, Canada
Edition: Unavailable
Pages: 35
Retrieved from: Critical Energy Infrastructure Protection Policy Research Series, No. 6: from the Carleton University website
Hyperlink: http://www3.carleton.ca/cciss/res_docs/ceip/hay.pdf
Date of Publication: March 2006

Objective:

- "The objective here is to explore and describe briefly the parts of the federal government that address the protection of critical energy infrastructure against acts of terrorism: which departments and agencies do what, how they interact with each other— and how they engage with the private industries that own (with provincial and territorial governments) some 85 per cent of Canadian energy infrastructure assets." [p. 3-4]

Description:

- "The exploration will start with an overview of energy infrastructure in Canada, with an eye to the complexities of sectoral and geographic differences.
- It will proceed to a quick chronology of policy and legislative events since 9/11, to help explain organizational structures as they evolved.
- It will then suggest a preliminary taxonomy of federal departments and agencies as they appeared in early 2006—and conclude with a set of issues worth further inquiry." [p. 3-4]

Additional Information:

- The author concludes, "in the end, it is not at all evident who in the government does exactly what to protect critical energy infrastructure"[p. 28].
- He provides three types of answers to explain this fact, then highlights the necessity to "seek a better understanding of who in the federal government ought to be doing what." [p. 29]

3.6.1.2 Critical Infrastructure Protection and the Role of Emergency Services

Title: Critical Infrastructure Protection and the Role of Emergency Services
Author(s): Mike Rothery (Assistant Secretary, Critical Infrastructure Protection Branch, Attorney-General's Department)
Organization: N/A
Publisher: Unavailable
Publishing Location: Australia
Edition: N/A
Pages: 6
Retrieved from: The Australian Journal of Emergency Management, Vol. 20, No. 2
Hyperlink: http://www.em.gov.au/Documents/Critical%20Infrastructure%20Protection.pdf
Date of Publication: May 2005

Description:

- This paper discusses the complexity of protecting critical infrastructure, and highlights the importance of building strong partnerships between the private sector and government. It places special emphasis on recognizing the emergency services as an essential component of Australia's critical infrastructure.
- This paper then describes the roles and activities of the following bodies:
    - The National Counter-Terrorism Committee and the Role of the States and Territories
    - Business-Government Task Force on Critical Infrastructure Protection
    - Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection
    - Infrastructure Assurance Advisory Groups
    - Critical Infrastructure Advisory Council
    - Owners and operators
    - The Attorney-General's Department
    - Emergency Services and the TISN

3.6.1.3 Critical Infrastructure Resilience: Whose Responsibility is it? (Fact Sheet)

Title: Critical Infrastructure Resilience: Whose Responsibility is it? (Fact Sheet)
Author(s): Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience
Organization: Trusted Information Sharing Network (TISN)
Publisher: Trusted Information Sharing Network (TISN)
Publishing Location: Australia
Edition: Unavailable
Pages: 2
Retrieved from: Trusted Information Sharing Network (TISN) website
Hyperlink: http://www.tisn.gov.au/Documents/CIR+-+Whose+Responsibility+is+it+-+Fact+Sheet.pdf
Date of Publication: Unavailable

Description:

- This fact sheet provides a very brief overview of critical infrastructure. It addresses the following questions:
  - What is critical infrastructure?
  - What are some examples of critical infrastructure?
  - What is critical infrastructure resilience?
- Next, the fact sheet discusses the role of the various actors who are responsible for critical infrastructure resilience. They are:
  - Owners and operators
  - State and territory governments
  - The Australian Government
  - The Trusted Information Sharing Network (TISN)

3.6.1.4 CRN Report - Focal Report 2 - Critical Infrastructure Protection

Title: CRN Report - Focal Report 2 - Critical Infrastructure Protection
Author(s): Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH (Swiss Federal Institute of Technology) Zürich
Organization: Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH (Swiss Federal Institute of Technology) Zürich
Publisher: Center for Security Studies (CSS), ETH Zürich
Publishing Location: Zürich, Switzerland
Edition: N/A
Pages: 24
Retrieved from: Centre for Security Studies (Switzerland) website
Hyperlink: http://www.css.ethz.ch/publications/pdfs/Focal-Report-2-CIP.pdf
Date of Publication: March 2009

Background:

- This is the second of two annual "focal reports"(Fokusberichte) produced by the Centre for Security Studies (CSS) at ETH Zürich.
- These reports aim to promote discussion and provide information regarding critical infrastructure protection and risk analysis.

Description:
This report is divided into two sections:

1. Critical Infrastructure Protection: Recent trends and developments
   "First, it identifies three trends in CIP based on the review of recently released policy and scientific documents (October 2008 to March 2009). This is followed by an annotated bibliography that continues to build upon the foundation laid in Focal Report 1. This section covers texts and resources for CIP in two sections: policy documents and academic texts." [p. 4]
2. The Meta-Governance of CIP
   "Second, the report highlights Public-Private Partnerships (PPPs) in the domain of CIP from a theoretical perspective. It draws on recent theories developed in public administration research, contributing to a better understanding of the associated challenges and potentials for cooperation between public and private actors. This main part is followed by a short selection of the most important academic literature in this domain." [p. 4]

3.6.1.5 The Flexibility Solution: How Private Enterprise Can Improve Infrastructure Security

Title: The Flexibility Solution: How Private Enterprise Can Improve Infrastructure Security
Author(s): Eli Lehrer and Wayne Crews
Organization: Competitive Enterprise Institute
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 4
Retrieved from: Competitive Enterprise Institute, No. 117, from the Competitive Enterprise Institute website
Hyperlink: http://cei.org/sites/default/files/Wayne%20Crews%20-%20The%20Flexibility%20Solution.pdf
Date of Publication: June 28, 2007

Background:

- "America has not done enough to protect the networks of roads, train lines, pipelines, power wires, ports, and fiber-optic networks that constitute the nation's critical infrastructure. This infrastructure, indeed, faces threats from all directions, from nuisances to existential risks…
- Over the last decade, government has taken an ever-growing role in providing this protection. Of course, government has a role to play in defending the country from threats both natural and man-made. But we will hurt our own security by allowing government's role to grow too large." [p. 1]

Description:

- "In this paper, we outline a new approach for protecting the nation, one that allows for the best use of both government and private efforts.
- We provide examples of how we might apply that framework to the Internet, to our air travel system, and to the nation's power grid. Good security against most threats requires flexibility, and private enterprise, on balance, provides greater flexibility than does government." [p. 1]

Additional Information:
This paper includes the following sections:

- Limits to Government's Role
- Government Rigidity vs. Private Flexibility
- New Strategies for Airline Security
- Electric Grid Security
- Conclusion

3.6.2 Information Sharing

3.6.2.1 Information Sharing and Protection under the Emergency Management Act

Title: Information Sharing and Protection under the Emergency Management Act
Author(s): Critical Infrastructure Policy, Emergency Management and National Security Branch, Department of Public Safety
Organization: Public Safety Canada
Publisher: Public Safety Canada
Publishing Location: Canada
Edition: Unavailable
Pages: 17
Retrieved from: Public Safety Canada website
Hyperlink: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/information-sharing-and-protection-under-the-ema-eng.pdf
Date of Publication: December 2007

Description:

- This document provides guidance on the Emergency Management Act's amendment to the Access to Information Act.

Additional Information:

- This amendment "allows the Government of Canada to protect specific critical infrastructure information supplied in confidence to the government by third parties. Private sector partners should note that critical infrastructure information can be protected under this exemption only if it is appropriately marked and is treated as confidential by the entity that provides the information. It should also be noted that exemptions from disclosure for reasons of national security and public safety already exist under federal/provincial/territorial access to and freedom of information legislation.
- The end result of these efforts to promote information sharing will be the development of a more coherent approach to emergency management at the national level and thereby ensure the maximum utility of the EMA." [p. 2]

3.6.2.2 Identifying and Marking Critical Infrastructure/Emergency Management (CI/EM) Information Shared in Confidence with the Government of Canada - Guide for Private Sector Entities

Title: Identifying and Marking Critical Infrastructure/Emergency Management (CI/EM) Information Shared in Confidence with the Government of Canada - Guide for Private Sector Entities
Author(s): Public Safety Canada
Organization: Public Safety Canada
Publisher: Public Safety Canada
Publishing Location: Ottawa, ON
Edition: Unavailable
Pages: 5
Retrieved from: Public Safety Canada website
Hyperlink: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/labelling-sensitive-cip-information-eng.pdf
Date of Publication: Unavailable

Purpose:

- "The purpose of this Guide is to provide general guidance for private sector entities to help them identify sensitive CI/EM information and develop specific markings for this information when it is shared in confidence with the Government of Canada." [p. 1]

Audience:

- "The information in this Guide is applicable to private sector entities who voluntarily share in confidence specific critical infrastructure/emergency management information with Government of Canada departments and agencies." [p. 1]

Additional Information:
This document provides guidance on the following topics:

- "Criteria the information must meet" [p. 2]
- "Marking CI/EM information provided in confidence to the Government of Canada" [p. 2]
- "Identifying specific CI/EM information shared in confidence" [p. 3]
- "*Access to Information Act* exemptions" [p. 4]
- "Sharing CI/EM information with the Government of Canada" [p. 5]
- "Transmitting CI/EM information shared in confidence with the Government of Canada " [p. 5]

3.6.2.3 Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors

Title: Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors
Author(s): United States General Accounting Office (GAO)
Organization: United States General Accounting Office (GAO)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 69
Retrieved from: GAO-04-780, Report to Congressional Requesters
Hyperlink: http://www.gao.gov/assets/250/243318.pdf
Date of Publication: July 2004

"Why GAO Did This Study

- Critical infrastructure protection (CIP) activities called for in federal policy and law are intended to enhance the security of the public and private infrastructures that are essential to our nation's security, economic security, and public health and safety. Effective information-sharing partnerships between industry sectors and government can contribute to CIP efforts. Federal policy has encouraged the voluntary creation of information sharing and analysis centers (ISAC) to facilitate infrastructure sector participation in CIP information sharing efforts.
- GAO was asked to identify actions that the Department of Homeland Security (DHS) could take to improve the effectiveness of CIP information-sharing efforts.

What GAO Recommends:

- GAO recommends that the Secretary of Homeland Security direct officials within DHS to (1) proceed with the development of an information-sharing plan that describes the roles and responsibilities of DHS, the ISACs, and other entities and (2) establish appropriate department policies and procedures for interactions with other CIP entities and for coordination and information sharing among DHS components.
- DHS commented on a draft of this report and generally agreed with our findings and recommendations." [Introductory Page]

3.6.2.4 National Infrastructure Protection Plan - Information Sharing

Title: National Infrastructure Protection Plan - Information Sharing
Author(s): Department of Homeland Security (DHS)
Organization: Department of Homeland Security (DHS)
Publisher: Department of Homeland Security (DHS)
Publishing Location: Unavailable
Edition: Unavailable
Pages: 2
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf
Date of Publication: Unavailable

Description:

- This document highlights the importance of information sharing for the effective implementation of the National Infrastructure Protection Plan (NIPP).
- It provides a brief overview of the progress made in improving information sharing under the NIPP and the Information Sharing Environment (ISE).

4 Incident Case Studies and Lessons Learned

Overview

This chapter provides references which describe specific incidents, how they affected or disrupted critical infrastructure, and the lessons learned. These references are divided according to the country or geographic area in which the incident occurred. The sections are as follows:

- Section 4.1: Canada
- Section 4.2: United States
- Section 4.3: United Kingdom
- Section 4.4: Australia
- Section 4.5: International

Within these sections, the references are ordered chronologically from most recent to least recent.

4.1 Canada

4.1.1 Ontario-U.S. Power Outage - Impacts on Critical Infrastructure

Title: Ontario-U.S. Power Outage - Impacts on Critical Infrastructure
Author(s): Public Safety and Emergency Preparedness Canada
Organization: Public Safety and Emergency Preparedness Canada
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 67
Retrieved from: Public Safety Canada website
Hyperlink: http://www.publicsafety.gc.ca/prg/em/_fl/ont-us-power-e.pdf
Date of Publication: August 2006

Purpose:

- "The purpose of this paper is to describe the Northeastern Interconnection power outage of August 14, 2003 and to identify how critical infrastructure was directly and interdependently impacted in Canada." [p. 1]

Audience:

- "This paper is intended to assist critical infrastructure protection and emergency management professionals in assessing the potential impacts of large-scale critical infrastructure disruptions and to encourage the private and public sectors to review their critical infrastructure protection and emergency management plans." [p. 1]

Additional Information:
This paper discusses the following:

- Background Information on Electric Power Grids
- Event description/Task Force Timeline
- Impact Timeline
- Affected Sectors:
    - Energy and Utilities
    - Communications
    - Services
    - Manufacturing
    - Transportation
    - Safety
    - Government
- Economic Impacts
- Conclusion

4.2 United States

4.2.1 Infrastructure Interdependencies Associated with the August 14, 2003, Electric Power Blackout

Title: Infrastructure Interdependencies Associated with the August 14, 2003, Electric Power Blackout
Author(s): Infrastructure Assurance Center, Argonne National Laboratory
Organization: Argonne National Laboratory
Publisher: Unavailable
Publishing Location: Argonne, IL, United States
Edition: Unavailable
Pages: 21
Retrieved from: Unavailable
Hyperlink: Unavailable
Date of Publication: August 29, 2003

Description:

- "This document briefly delineates and synopsizes the impacts of the August 14, 2003, blackout on other critical infrastructures dependent on electric service. (These reported impacts reflect infrastructure interdependencies.)
- It is not intended to be a comprehensive study but rather a quick look at critical infrastructures and key assets in the U.S. (and, to a lesser extent, Canada) that contains representative examples of impacts reported by the news media." [p. 2]

Additional Information:
The affected infrastructures that are discussed in this report are:

- Energy
- Chemical Industry and Hazardous Materials
- Water
- Agriculture and Food
- Public Health
- Emergency Services
- Defense Industrial Base
- Information and Telecommunications
- Transportation
- Banking and Finance
- Postal and Shipping
- Other

4.2.2 Effects of Catastrophic Events on Transportation System Management and Operations - Cross Cutting Study

Title: Effects of Catastrophic Events on Transportation System Management and Operations - Cross Cutting Study
Author(s): U.S. Department of Transportation's John A. Volpe National Transportation Systems Centre
Organization: U.S. Department of Transportation
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 63
Retrieved from: Research and Innovative Technology Administration, National Transportation Library website
Hyperlink: http://ntl.bts.gov/lib/jpodocs/repts_te/13780_files/13780.pdf
Date of Publication: January 2003

Description:

- "In order to provide a better understanding of how transportation is both affected and utilized in an emergency situation, the Federal Highway Administration (FHWA) commissioned a series of four case studies examining the effects of catastrophic events on transportation system management and operations. Each of the case studies examined a specific event and the regional response.
- The events included terrorist attacks in New York City and Washington, D.C., on September 11, 2001; an earthquake in the Los Angeles region; and a rail tunnel fire in Baltimore.
- This cross cutting study summarizes the surface transportation activities associated with four catastrophic events and the lessons learned from each. Each of the events resulted in substantial, immediate, and adverse impacts on the transportation system, and each has had a varying degree of influence on the longer-term operation of transportation facilities and services in its respective region." [p. iii]

4.2.3 Homeland Security - Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview

Title: Homeland Security - Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview
Author(s): Jeffrey W. Seifert (Analyst in Information Science and Technology Policy; Resources, Science and Industry Division)
Organization: Congressional Research Service
Publisher: Congressional Research Service
Publishing Location: Washington D.C.
Edition: Unavailable
Pages: 26
Retrieved from: Congressional Research Service Report CRS-RL31542, retrieved from the Federation of American Scientists website
Hyperlink: http://www.fas.org/sgp/crs/RL31542.pdf
Date of Publication: Updated December 12, 2002

Description:

- "This report assesses the impact of the September 11, 2001 attacks on public and private information infrastructures in the context of critical infrastructure protection, continuity of operations (COOP) planning, and homeland security. Analysis of the effects of the terrorist attacks suggests various "lessons learned"." [Summary page]

Additional Information:

- This report places special emphasis on the lessons learned from the September 11 attacks. The lessons apply to continuity and disaster recovery planning, and can assist policymakers and businesses in the development and implementation of new initiatives for homeland security.
- These lessons support three general principles. They are:
    - Continuity and Recovery Planning and Practices
    - Decentralization
    - Redundancy and Planning of Communications
- This report also discusses future considerations in the area of business continuity as well as information sharing and collaboration.

4.2.4 Incident Analysis: The September 11, 2011 Terrorist Attacks - Critical Infrastructure Protection Lessons Learned

Title: Incident Analysis: The September 11, 2011 Terrorist Attacks - Critical Infrastructure Protection Lessons Learned
Author(s): Office of Critical Infrastructure Protection and Emergency Preparedness
Organization: Office of Critical Infrastructure Protection and Emergency Preparedness
Publisher: Office of Critical Infrastructure Protection and Emergency Preparedness
Publishing Location: Canada
Edition: Unavailable
Pages: 23
Retrieved from: Incident Analysis, Number IA02-001, from the Public Safety website
Hyperlink: http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/ia02-001-eng.pdf
Date of Publication: 27 September 2002

Description:

- "In the year following the September 11 terrorist attacks on the World Trade Center and the Pentagon a number of documents have been compiled that analyze the impact, response and outcomes that stem from the attacks.
- This report has been compiled to assist Canadian critical infrastructure (CI) owners and operators with their business continuity planning and emergency management (EM) preparations by identifying critical infrastructure protection (CIP) and EM lessons that can be learned from these tragic events.
- The analysis is based on open source information and feedback provided by CIP and EM partners. A selected list of lessons learned reports regarding the September 11 attacks has been included at the end of the document." [Executive Summary]

Additional Information:

- "This report will identify lessons learned from the attacks that could be applied to five sectors of critical infrastructure (CI): communications, transportation, energy, banking and finance, and government.
- Following a brief description of the attacks, each sector will be examined in turn for general CIP lessons that can be drawn from specific instances relating to the terrorist attacks.
- The lessons have not been ranked according to importance and readers are encouraged to peruse the document in its entirety as lessons cited for one sector can often assist with CIP/EM efforts in another sector." [p. 1]

4.3 United Kingdom

4.3.1 Learning Lessons from the 2007 Floods

Title: Learning Lessons from the 2007 Floods
Author(s): Pitt Review: Sir Michael Pitt (Independent Chair), and the Review Team
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 505
Retrieved from: UK Government National Archives website
Hyperlink:
http://webarchive.nationalarchives.gov.uk/20100807034701/http:/archive.cabinetoffice.gov.uk/pittreview/thepittreview/final_report.html
Date of Publication: 25 June 2008

Description:

- This publication provides a comprehensive review of the lessons learned from the summer floods of 2007. It outlines and elaborates on the six major lessons learned. They are:
  - "Knowing where and when it will flood
  - Reducing the risk of flooding and its impact
  - Being rescued and cared for during an emergency
  - Maintaining power and water supplies and protecting essential services
  - Better advice and help for people to protect their families and homes
  - Staying healthy and speeding up recovery." [p. viii]
- A key component of this report are the recommendations, which provide direction for changes in the way the United Kingdom should prepare for, respond to, and recover from flooding.

4.3.2 The United Kingdom Foot and Mouth Disease Crisis - Impact on Critical Infrastructure

Title: The United Kingdom Foot and Mouth Disease Crisis - Impact on Critical Infrastructure
Author(s): Unavailable
Organization: Unavailable
Publisher: Public Safety Canada
Publishing Location: Unavailable
Edition: Unavailable
Pages: N/A
Retrieved from: Incident Analysis, IA06-001, from the Public Safety website
Hyperlink: http://www.publicsafety.gc.ca/prg/em/ccirc/2006/ia06-001-eng.aspx
Date of Publication: 26 May 2006

Purpose:

- "Using the 2001 Foot and Mouth Disease (FMD) outbreak in the United Kingdom (UK) as a case study, this paper provides an illustration of how a contagious animal disease can affect critical infrastructure (CI). It also provides background information on FMD and the 2001 outbreak. Canadian CI sector stakeholders can use this analysis to gain a perspective of the overall negative effects that can result from an outbreak of FMD"[9].

Audience:

- "This incident analysis is intended for people who work in the transportation, communications and information technology, food, government and safety sectors"[10].

Description:

- "In recent years, the threat of Foot and Mouth Disease (FMD) (also known as Hoof and Mouth Disease) has been at the forefront of public and private sector interest due to its proven crippling effects on sectors critical to a country's prosperity, specifically the economy and the tourism industry. As a result of this interest, several reports have been released discussing how FMD outbreaks can cause significant damage to these sectors.
- This report focuses on how FMD adversely affected other CI sectors. The CI sectors examined in this paper are: transportation, communications and information technology, food, government and safety…
- The information in this impact assessment was derived from open-source media and government material, including the UK inquiry report entitled *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry Report*, published on July 22, 2002. The Canadian Food Inspection Agency, Health Canada and the UK Civil Contingencies Secretariat were consulted in the writing of this paper"[11].

[9] From http://www.publicsafety.gc.ca/prg/em/ccirc/2006/ia06-001-eng.aspx
[10] Ibid.
[11] Ibid.

4.4 Australia

4.4.1 Australian Critical Infrastructure Protection: A Case of Two Tales

Title: Australian Critical Infrastructure Protection: A Case of Two Tales
Author(s): Matthew Warren (Deakin University), Graeme Pye (Deaken University), William Hutchinson (Edith Cowan University)
Organization: Edith Cowan University
Publisher: Edith Cowan University
Publishing Location: Unavailable
Edition: N/A
Pages: 30-36
Retrieved from: Proceedings of the 11th Australian Information Warfare Conference, Edith Cowan University, Perth Western Australia, 30th November - 2nd December 2010
Hyperlink: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1035&context=isw
Date of Publication: 2010

Abstract:
"The protection of critical infrastructures and the choices made in terms of priorities and cost, all impact upon the planning, precautions and security aspects of protecting these important systems. Often the when choices made is difficult to assess at the time the decision is taken and it is only after an incident that the truth of the choices made become fully evident. The paper focuses on two recent examples of Australian Critical Infrastructure protection and the issues that related to those examples." [p. 30]

Keywords: Australia; Critical Infrastructure Protection; Risk.

Description:
- This paper uses two case studies to illustrate key issues that arise in the area of critical infrastructure protection. It places special emphasis on the need for decision makers to be aware of these issues when making choices related to critical infrastructure and security.
- The case studies are drawn from the Victorian Bushfires of 2009.
    - The first case study covers the impact of the Victorian bushfires on environmental security, or more specifically, water supply. This case study highlights the dangers that natural hazards can pose to critical infrastructure.
    - The second case study provides an example in which critical infrastructure was the cause of disruption and loss of property and life.

4.5 Multi/International

4.5.1 Microsoft SQL Server 2000 "Slammer" Worm - Impact Paper

Title: Microsoft SQL Server 2000 "Slammer" Worm - Impact Paper
Author(s): Office of Critical Infrastructure Protection and Emergency Preparedness
Organization: Office of Critical Infrastructure Protection and Emergency Preparedness
Publisher: Office of Critical Infrastructure Protection and Emergency Preparedness
Publishing Location: Canada
Edition: Unavailable
Pages: 13
Retrieved from: Incident Analysis, Number IA03-001, from the Public Safety website
Hyperlink: http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/ia03-001-eng.pdf
Date of Publication: 12 March 2003

Purpose:

- "This paper will examine the impact of the SQL Server 2000 “Slammer” worm on global critical infrastructure (CI) elements. The information in this paper could be used to illustrate how interdependent CI elements in disparate industry sectors have become increasingly underpinned by networked computer technologies." [p. 1]

Audience:

- "This paper has been written in order to assess the scope and impact of the Slammer worm. As such, it is primarily intended for CI stakeholders who rely on computer network technologies for their enterprises." [p. 1]

Description:

- After providing an introduction, background information, and a description of the outbreak, this paper discusses the impacts of the Slammer worm on critical infrastructure sectors.
  The affected sectors are:
  - Banking & Financial Services;
  - Telecommunications;
  - Energy & Utilities;
  - Safety & Emergency Services;
  - Transportation;
  - Government Services;
  - Additional Economic Impacts

Additional Information:

- The paper concludes by stating, "the worm served to highlight the importance of having properly configured perimeter defences to protect internal services that should not be accessible from the Internet, as well as the value of maintaining a defensive posture regarding emerging vulnerabilities. Users who had taken these steps experienced a greatly reduced impact from the worm." [p. 11]

5 Business Continuity

Overview

This chapter includes references on business continuity management (BCM). Although BCM is a necessary component of critical infrastructure management, there have been few attempts to integrate the two approaches. Thus, the BCM references have been separated from the other processes for managing CI, in order to reflect the disassociation that currently exists in the literature. This chapter is divided into the following:

- Section 5.1: BCM standards
- Section 5.2: frameworks and guidelines for BCM
- Section 5.3: miscellaneous references on business continuity

Within each section, similar references are grouped, then ordered from most to least recent.

5.1 Standards

5.1.1 ISO 22301 Societal Security - Business Continuity Management Systems - Requirements

Title: ISO 22301 Societal Security - Business Continuity Management Systems - Requirements
Author(s): Technical Committee ISO/TC 223, Societal Security
Organization: International Organization for Standardization (ISO)
Publisher: International Organization for Standardization (ISO)
Publishing Location: Switzerland
Edition: 1st ed.
Pages: 34
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: May 2012

General:

- "This International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS)." [p. v]

Scope:

- "This International Standard for business continuity management specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
- The requirements specified in this International Standard are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.
- It is not the intent of this International Standard to imply uniformity in the structure of a Business Continuity Management System (BCMS), but for an organization to design a BCMS that is appropriate to its needs and that meets its interested parties' requirements…
- This International Standard can be used to assess an organization's ability to meet its own continuity needs and obligations." [p. 1]

Additional information:
This standard includes:

- Definitions
- Requirements for the essential elements of the Business Continuity Management System. These elements are:
    - Context of the organization
    - Leadership
    - Planning
    - Support
    - Operation
    - Performance Evaluation
    - Improvement

5.1.2 CSA Z1600-08 Emergency Management and Business Continuity Programs

Title: CSA Z1600-08 Emergency Management and Business Continuity Programs
Author(s): Technical Committee on Emergency Management and Business Continuity, Canadian Standards Association
Organization: Canadian Standards Association
Publisher: Canadian Standards Association
Publishing Location: Mississauga, Ontario, Canada
Edition: 1st ed.
Pages: 50
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: August 2008

Purpose:

- "This new Canadian Standard outlines the requirements for a comprehensive emergency management program. The goal of this Standard is to establish the elements of a continuous improvement process to develop, implement, maintain, and evaluate emergency management and business continuity programs that address the functions of prevention and mitigation, preparedness, response, and recovery." [p. viii]

Scope:

- "The Standard establishes a common set of criteria for emergency management and business continuity programs.
- This Standard establishes the elements of a continuous improvement process to develop, implement, maintain, and evaluate emergency management and business continuity programs that address prevention and mitigation, preparedness, response, and recovery. The elements of a continuous improvement process included in this Standard are:
    a. Program management;
    b. Planning;
    c. Implementation;
    d. Evaluation; and
    e. Management review
- This Standard covers programs in which the functions of prevention and mitigation, preparedness, response, and recovery are considered independently or in combinations.
- The elements of programs covered by this Standard address the functions (prevention and mitigation, preparedness, response, and recovery) commensurate with the risks established by the entity's hazard identification, risk assessment, and business impact analysis.
- This Standard applies to public, not-for-profit, and private entities." [p. 1]

Additional Information:

- This Canadian Standard was developed by using and adapting the National Fire Protection (NFPA)'s NFPA 1600, *Standard on Disaster/Emergency Management and Business Continuity Programs (2007)*

5.1.3 NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs

Title: NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs
Author(s): Technical Committee on Emergency Management and Business Continuity
Organization: National Fire Protection Association (NFPA)
Publisher: Unavailable
Publishing Location: United States of America
Edition: 2010 ed.
Pages: 52
Retrieved from: NFPA website
Hyperlink: http://www.nfpa.org/assets/files//PDF/NFPA16002010.pdf
Date of Publication: 2010

Purpose:
- "This standard provides the fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery." [p. 5]

Scope:
- "This standard shall establish a common set of criteria for all hazards disaster/emergency management and business continuity programs...
- This document shall apply to public, not-for-profit, non-governmental organizations (NGO), and private entities on a local, regional, national, international, and global basis." [p. 5]

Description:
This Standard establishes criteria for each of the essential components of the disaster/emergency management and business continuity programs. These components are:
- Program management
- Planning
- Implementation
- Testing and exercises
- Program improvement

Additional Information:
- This Standard also includes a tool which allows users to assess their conformity with NFPA 1600.
- This Standard was approved as an American National Standard by the American National Standards institute.

5.1.4 Professional Practices for Business Continuity Practitioners

Title: Professional Practices for Business Continuity Practitioners
Author(s): Disaster Recovery Institute (DRI) International
Organization: Disaster Recovery Institute (DRI) International
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 47
Retrieved from: Disaster Recovery Institute (DRI) International website
Hyperlink: https://www.drii.org/docs/profprac_details.pdf
Date of Publication: July 2008

Description:

- These standards present a framework for a Business Continuity Management (BCM) Program.
- The standards also describe the role of business continuity practitioners. Using the 10 components of the BCM Program as a guideline, it highlights action areas in which practitioners should demonstrate working knowledge in order to effectively implement a BCM Program.

Additional Information:

- The 10 components of the Business Continuity Management Program are:
    - "Program Initiation and Management...
    - Risk Evaluation and Control...
    - Business Impact Analysis...
    - Business Continuity Strategies...
    - Emergency Response and Operations...
    - Business Continuity Plans...
    - Awareness and Training Programs...
    - Business Continuity Plan Exercise, Audit and Maintenance
    - Crisis Communications...
    - Coordination with External Agencies" [p. 3-4]
- These components "are not presented in any particular order of importance or sequence, as it may be necessary to undertake or implement sections in parallel during the development of the BCM Program." [p. 3]

5.1.5 Generally Accepted Practices for Business Continuity Practitioners

Title: Generally Accepted Practices for Business Continuity Practitioners
Author(s): Disaster Recovery Journal and Disaster Recovery Institute (DRI) International
Organization: Disaster Recovery Journal and Disaster Recovery Institute (DRI)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 163
Retrieved from: Disaster Recovery Journal website
Hyperlink: http://www.drj.com/GAP/gap.pdf
Date of Publication: August 2007

Mission Statement:

- "To be recognized as a leading source of "sound" Generally Accepted Practices by providing a depository of knowledge and recommendations offered by skilled Business Continuity Professionals." [p. 4]

Description:

- This document is a supplement to "Professional Practices for Business Continuity Practitioners".
- Whereas "Professional Practices for Business Continuity Practitioners" outlines what a professional should do, this document describes how these actions can be carried out.

Additional Information:

- The descriptions in this document align with the 10 components, or subject areas that are outlined in "Professional Practices for Business Continuity Practitioners". These areas are:
  - Program Initiation and Management
  - Risk Evaluation and Control
  - Business Impact Analysis
  - Business Continuity Strategies
  - Emergency Response and Operations
  - Business Continuity Plans
  - Awareness and Training Programs
  - Business Continuity Plan Exercise, Audit and Maintenance
  - Crisis Communications
  - Coordination with External Agencies
- This document outlines sub-topics for each of the above components. For each sub-topic, this document describes what should be done and how. In addition, it provides references to potential resources.

5.2 Frameworks and Guidelines

5.2.1 A Guide to Business Continuity Planning

Title: A Guide to Business Continuity Planning
Author(s): Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada
Organization: Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 21
Retrieved from: Government of Manitoba website
Hyperlink: http://www.gov.mb.ca/emo/home/bcont_e.pdf
Date of Publication: Unavailable

Description:

- "This publication provides a summary and general guidelines for Business Continuity Planning (BCP)." [p. 1]

Additional Information:
This guide is broken down into the following sections:

- Section 1: Introduction
  - Overview
  - Changes in the World of Business Continuity Planning
- Section 2: Creating a Business Continuity Plan (5 components)
  - Establish Control
  - Business Impact Analysis
  - Plans for Business Continuity
  - Readiness Procedures
  - Quality Assurance Techniques
- Section 3: What to do when a Disruption Occurs
  - Response
  - Continuation
  - Recovery and Restoration

**Note*: This document is also available on the Public Safety Canada website at http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx

5.2.2 Business Continuity Guide

Title: Business Continuity Guide
Author(s): Business Continuity Planning Section, Alberta Emergency Management Agency
Organization: Alberta Municipal Affairs & Housing, and Alberta Emergency Management Agency
Publisher: Alberta Emergency Management Agency
Publishing Location: Edmonton, Alberta
Edition: 2nd ed.
Pages: 208
Retrieved from: Alberta Emergency Management Agency
Hyperlink: http://www.aema.alberta.ca/documents/bcp_guide_March_2007.pdf
Date of Publication: March 2007

Purpose:

- "This document will assist Business Continuity Managers and their teams through the process of business continuity planning and management. The Planning Guide provides a step-by-step guide for all facets of business continuity planning. It can be applied to any department, division, branch and section level (and their equivalencies). The guide can also be applied to private industry as required.
- This guide does not include specific details of the various components of business continuity planning but rather is an overview. Although the Planning Guide has a generic format, some of its content may not be applicable to all organizations. Users are encouraged to amend components of this guide to meet the needs of their organization. Additional information and assistance is available from the Business Continuity Planning Section of the Alberta Emergency Management Agency (AEMA)." [p. 19]

Audience:

- "The Business Continuity Guide has been written for the Government of Alberta; by employees of the Government; emphasizing the responsibility to resume essential services for Albertans in the face of emergencies, disasters and disruptions." [p. 3]

Description:

- The "Business Continuity Guide currently consists of five modules:
  - Part 1 – Planning Guide
  - Part 2 – Business Continuity Plan Template
  - Part 3 – Training and Awareness
  - Part 4 – Exercising and Validation
  - Part 5 – Performance Measures
- Each module includes multiple annexes to support a business continuity plan." [p. 3]

5.2.3 Business Continuity Management Planning Guidelines 2006

Title: Business Continuity Management - Planning Guidelines 2006
Author(s): Government of Saskatchewan
Organization: Government of Saskatchewan
Publisher: Government of Saskatchewan
Publishing Location: Saskatchewan
Edition: Version 06.1 (March 2006)
Pages: 101
Retrieved from: Saskatchewan Research Council website
Hyperlink: http://www.src.sk.ca/images/Business%20Continuity%20Planning%20Guide%20-%20v%2006%201%20online%20version.pdf
Date of Publication: 2006

Objective:

- "The objective of this guide is to provide a consistent approach to Business Continuity plan development within the government.
- All government departments and agencies are encouraged to adopt this guide in developing their departmental plan so that there is a uniform and consistent process in Business Continuity Management in government." [p. ii]

Audiences:

- "The principles in these guidelines are applicable to all organizations of any size, sector and location – from those with a single site to those with multiple and remote locations. The approach taken in development included research of other jurisdictions' experiences and industry best practices in business continuity planning.
- These guidelines are intended for use by designated department or agency Business Continuity planners, risk managers, auditors and regulators. It is recommended that newcomers to the discipline attend an appropriate selection of the many endorsed Business Continuity Management courses or work alongside an experienced practitioner." [p. ii]

Scope:

- The Guidelines focus "on the primary role of the BCM practitioner and assume that specialist in other disciplines (IT, Security, HR, Finance and Facilities etc.) will be available to advise on the implementation of these aspects." [p. 3]

Description:

- These guidelines outline and describe business continuity management and its components. It also suggests methods to effectively implement the process.

Additional Information:
This guide includes the following sections:

- Business Continuity management Overview
- Business Continuity Management Program
- Business Continuity Responses
- Business Continuity Implementation Components
- Business Continuity Sustaining Components

5.2.4 Business Continuity Planning Workbook 2006

Title: Business Continuity Planning Workbook 2006
Author(s): Government of Saskatchewan
Organization: Government of Saskatchewan
Publisher: Government of Saskatchewan
Publishing Location: Unavailable
Edition: Version 06.1
Pages: 30
Retrieved from: Saskatchewan Research Council Website
Hyperlink:
http://www.src.sk.ca/images/GoS%20BCP%20Workbook%20%20v%2006%201%20online%20version.pdf
Date of Publication: 2006

Description:

- "To supplement the Government of Saskatchewan Business Continuity Management Planning Guidelines, the Government of Saskatchewan Business Continuity Planning Workbook has been developed to assist business units with creating mission critical specific plans to ensure the restoration of business, operations and departmental support after a disruptive event." [p. 1]

Additional Information:
This workbook provides tables, templates, rating criteria and/or checklists to guide users through each of the following steps:

- Continuity planning development
- Identify Mission Critical Functions
- Complete the Business Impact Analysis
- Perform a Threat Risk Assessment
- Prioritize Mission Critical Functions
- Developing Business Continuity Strategies
- Identify Mission Critical Resource Requirements
- Identify Vital Records
- Complete an Internal and External Contact List
- Write the Plan
- Tabletop Exercise

5.2.5 Business Continuity Management Guideline

Title: Business Continuity Management Guideline
Author(s): Autorité des marchés financiers
Organization: Autorité des marchés financiers
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 16
Retrieved from: Autorité des marchés financiers website
Hyperlink: http://www.lautorite.qc.ca/files/pdf/reglementation/lignes-directrices-toutes-institutions/2010mars31-ld-gestion-continuite-en.pdf
Date of Publication: April 2010

Scope:

- "This guideline applies to financial institutions operating independently as well as to financial institutions operating as members of a financial group." [p. 5]

Audience:

- "This business continuity management guideline is intended for insurers of persons (life and health), damage insurers, portfolio management companies controlled by an insurer, guarantee funds, mutual insurance associations, financial services cooperatives as well as trust and savings companies." [p. 5]

Description:

- "This guideline sets out the expectations of the AMF regarding business continuity management. Under the various sector-based laws it administers, the AMF has the authority to establish guidelines regarding sound and prudent management practices for financial institutions." [p. 4]

Additional Information:

- This document provides general guidance on:
    - Coming into effect and updating
        i. Continuity and resumption of business
        ii. Sound and prudent business continuity management
        iii. General framework for business continuity management
        iv. Identification and analysis of major operational incidents
        v. Development and implementation of the business continuity plan
    - Supervision of sound and prudent management practices
- In addition, this guideline provides 7 principles which support the business continuity management process.

5.2.6 Business Continuity Management Practice Guide

Title: Business Continuity Management Practice Guide
Author(s): Financial Service Authority (FSA)
Organization: Financial Service Authority (FSA)
Publisher: Unavailable
Publishing Location: United Kingdom
Edition: Unavailable
Pages: 38
Retrieved from: Financial Service Authority (FSA) website
Hyperlink: http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf
Date of Publication: November 2006

Purpose:

- "The Business Continuity Management Practice Guide is not general guidance from the Tripartite Authorities, nor is it guidance on FSA rules. Rather, it aims to help regulated firms in their business continuity planning by identifying and sharing examples of business continuity practice observed in firms that participated in the benchmarking exercise. We hope that these observations may be useful for firms when reviewing their own business continuity and crisis management arrangements.
- Firms should not view the Guide as a definitive checklist of steps to take, but rather as a flexible tool to stimulate their thinking and provide a framework for the development of their own plans. Above all else, firms should continue to be mindful of their individual circumstances and risk profiles when considering what may – or may not – be appropriate for their business." [p. 1-2]

Description:

- This guide identifies observed standard practices and observed leading practices in the following areas:
  - "Corporate Continuity
  - Corporate Crisis Management
  - Corporate Systems
  - Corporate Facilities
  - Corporate People" [p. 2]
- This information is presented in a series of charts.

5.2.7 Business Continuity Management - Building Resilience in Public Sector Entities

Title: Business Continuity Management - Building resilience in Public Sector Entities
Author(s): Australian National Audit Office
Organization: Australian National Audit Office
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 148
Retrieved from: Australian National Audit Office website
Hyperlink: http://www.anao.gov.au/uploads/documents/Business_Continuity_Management_.pdf
Date of Publication: June 2009

Description:

- This document is a "better practice guide." [p. 1]
- This publication is divided into two sections:
  - The Guide: Provides explanations, points for consideration, case studies, checkpoints and further references for business continuity management.
  - Workbook: Provides examples, templates, and checklists.

Additional Information:

- Both the Guideline and the Workbook are structured in accordance with the Australian National Audit office's elements of a better practice business continuity management program. These elements are:
  - "Managing business continuity as an integrated program of work
  - Embedding business continuity management into the entity's culture
  - Analysing the entity and its context
  - Designing the entity's business continuity approach
  - Building entity resilience
  - In the event of a disruption: Activating and deploying the plan
  - Maintaining the program and plan: Testing, exercising, updating and reviewing" [p. 1]

**Note*: This document is not available in pdf form, but is viewable as an ebook at http://www.anao.gov.au/uploads/documents/Business_Continuity_Management_.pdf

5.2.8 Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies

Title: Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies
Author(s): Annabelle Boyd, Jim Caton, and Anne Singleton (Boyd, Caton & Grant Transportation Group), and Peter Bromley and Chuck Yorks (McCormick Taylor, Inc.)
Organization: Transportation Research Board (TRB) of the National Academies
Publisher: National Academies of Science
Publishing Location: Washington, D.C.
Edition: Unavailable
Pages: 74
Retrieved from: Transportation Research Board's National Cooperative Highway Research Program (NCHRP) Report 86, Vol. 8 and the Transportation Research Board's Transit Cooperative Research Program (TCRP) Report 525, Vol. 8
Hyperlink: http://www.trb.org/Main/Blurbs/156474.aspx>
Date of Publication: 2005

Objective:

- "The objective of Volume 8: Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies is to provide guidelines for state and local transportation agencies to develop, implement, maintain, train for, and exercise COOP capabilities. " [p. vii]

Audience:

- "The guidelines are expected to be applied by designated agency continuity planners using templates to customize COOP plans for their local conditions." [p. vii]

Description:

- "These guidelines discuss recommended content for a transportation agency COOP plan. After a brief introduction and description of existing federal requirements for COOP planning, these guidelines cover the following topics:
    - Starting COOP planning;
    - Identifying system capabilities to deal with emergencies and vulnerabilities within the agency;
    - Identifying essential functions of the agency;
    - Identifying key personnel, delegations of emergency authority, and orders of succession;
    - Determining vital records, systems, and equipment and a process to safeguard and update these items;
    - Evaluating needs and selecting an alternate work site;
    - Developing an effective interoperable communications plan; and
    - Testing and executing the COOP plan and revising it periodically as necessary." [p. 1]

5.3 Miscellaneous

5.3.1 Multicriteria Decision Support for Business Continuity Planning in the Event of Critical Infrastructure Disruptions

Title: Multicriteria Decision Support for Business Continuity Planning in the Event of Critical Infrastructure Disruptions
Author(s): Merz, M., Hiete, M., Bertsch, V.
Organization: University of Karlsruhe (TH), Institute for Industrial Production (IIP), Germany
Publisher: Inderscience Enterprises Ltd.
Publishing Location: Switzerland
Edition: N/A
Pages: 156-174
Retrieved from: International Journal of Critical Infrastructures, vol. 5, no. 1-2
Hyperlink: N/A
Date of Publication: 2009

Abstract:
"Industrial production sites and Critical Infrastructures (CIs) may be severely damaged by external events, such as man-made or natural hazards. Particularly, a disruption in the electricity supply may cause physical damages and production downtimes associated with substantial economic losses. Due to the tight interdependencies within the different CI sectors and the complex network structure of modern supply chains, these losses are (in most cases) not restricted to single companies and the resultant negative consequences might be propagated via cascading effects into far-off supply chain links. In order to reduce the negative consequences, speed up business recovery and enhance the overall coping capacity of industrial production sites and global supply chains in the event of CI disruptions, many companies have implemented Business Continuity Planning (BCP) programmes. Within this study, we assess the negative impacts of CI disruptions on production industry and introduce a quantitative method for BCP from the field of Multicriteria Decision Analysis (MCDA) to evaluate the potential BCP measures." [p. 156]

Key words: business continuity planning; BCP; multicriteria decision analysis; MCDA; critical infrastructures; supply disruptions; industrial crisis management

Objective:
- "The main objective of this paper is to present a structure approach for industrial crisis management for the level of production sites, which should enable fast business recovery and business continuity in the industries affected by natural disasters or CI disruptions." [p. 157]

Additional Information:
"The paper is structured as follows.
- In Section 2, after presenting the general aspects of supply chain risks and pointing out the importance of CI, the impacts of natural hazards and CI disruptions on industrial production sites are described.
- In Section 3, selected topics of crisis management for supply chain disruptions, e.g., business recovery and Business Continuity Planning (BCP), are addressed.
- In Section 4, a quantitative method for BCP from the field of multicriteria decision support is introduced.
- Its application in a case study is presented in Section 5.
- The conclusions of the paper are drawn in Section 6." [p. 157-158]

5.3.2 Survey and Assessment of Planning for Operational Continuity in Public Works

Title: Survey and Assessment of Planning for Operational Continuity in Public Works
Author(s): Scott Somers (Arizona State University - Polytechnic Campus)
Organization: N/A
Publisher: Sage Publications
Publishing Location: Unavailable
Edition: N/A
Pages: 451-465
Retrieved from: Public Works Management & Policy, Vol. 12, No. 2
Hyperlink: http://pwm.sagepub.com/content/12/2/451.full.pdf
Date of Publication: October 2007

Abstract:
"The public works department provides an array of essential services to the community that business and citizens rely on. Preparation for service provision during and after a crisis is called continuity of operations planning (COOP).Historically, the federal government has conducted such planning, and private businesses have embraced business continuity planning. Local governments have more recently begun to adopt such "good business practices." This article provides a background on government COOP planning, describes the important elements of a continuity plan as described in federal documents and standards, and reports on a survey of public works departments. The results of the survey indicate that although some planning efforts have been undertaken, a majority of public works agencies in this sample are at risk for breakdowns in the provision of essential service in crisis situations. Public works agencies need to intensify planning efforts to ensure operational continuity." [p. 451]

Description:

- "This article addresses the issue of planning to reduce or minimize service disruptions to critical municipal lifeline services provided by public works departments.
- The premise is that public works agencies must have structural and personnel integrity to maintain service delivery in the face of an unexpected event.
- The data presented here characterize the extent to which public works departments have attended to COOP plan elements that would enhance the level of operational continuity during disaster. This data was collected in a survey of public works agencies in the southwest United States. Information on the extent of COOP plan adoption alerts public works managers and community emergency planners to the issue of operational continuity, identifies important COOP plan elements, and provides basic information for assessing organizational preparedness. Such information provides a useful snapshot of current COOP planning activities and can be used as a tool to evaluate the vulnerability of public works departments to service disruptions." [p. 452]

5.3.3 Continuity of Operations/Continuity of Government for State-Level Transportation Organizations

Title: Continuity of Operations/Continuity of Government for State-Level Transportation Organizations
Author(s): Frances L. Edwards, Daniel C. Goodrich
Organization: Mineta Transportation Institute
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 684
Retrieved from: Mineta Transportation Institute (MTI) Report 11-02
Hyperlink: http://www.transweb.sjsu.edu/PDFs/research/2976-COOP-COG-DHS.pdf
Date of Publication: September 2011

Abstract:
"The Homeland Security Presidential Directive 20 (HSPD-20) requires all local, state, tribal and territorial government agencies, and private sector owners of critical infrastructure and key resources (CI/KR) to create a Continuity of Operations/Continuity of Government Plan (COOP/COG). There is planning and training guidance for generic transportation agency COOP/COG work, and the Transportation Research Board has offered guidance for transportation organizations. However, the special concerns of the state-level transportation agency's (State DOT's) plan development are not included, notably the responsibilities for the entire State Highway System and the responsibility to support specific essential functions related to the State DOT Director's role in the Governor's cabinet. There is also no guidance on where the COOP/COG planning and organizing fits into the National Incident Management System (NIMS) at the local or state-level department or agency. This report covers the research conducted to determine how to integrate COOP/COG into the overall NIMS approach to emergency management, including a connection between the emergency operations center (EOC) and the COOP/COG activity. The first section is a presentation of the research and its findings and analysis. The second section provides training for the EOC staff of a state-level transportation agency, using a hybrid model of FEMA's ICS and ESF approaches, including a complete set of EOC position checklists, and other training support material. The third section provides training for the COOP/COG Branch staff of a state-level transportation agency, including a set of personnel position descriptions for the COOP/COG Branch members." [p. ii]

5.3.4 Integrating Measures for Business Continuity and TDM [Transportation Demand Management] to Ensure Regional Emergency Preparedness and Mobility

Title: Integrating Measures for Business Continuity and TDM [Transportation Demand Management] to Ensure Regional Emergency Preparedness and Mobility
Author(s): Frank Mongioi, Lisa McNally, Ryan Thompson
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 85-94
Retrieved from: Transportation Research Record: Journal of the Transportation Research Board, 2137
Hyperlink: http://www.trforum.org/forum/downloads/2009_12_TDMMeasures_paper.pdf
Date of Publication: 2009

Abstract

"The business community must be prepared for a variety of emergencies ranging from natural disasters to terrorist attacks. Additionally, businesses have to be prepared to continue operations with the expectation that it may not be business as usual. For businesses, protection of critical resources is paramount in emergency planning. However, the consideration of employee mobility during and after an emergency is less often considered, although it is an equally significant aspect of businesses continuity.

The objective of this paper is to explore how Metropolitan Planning Organizations (MPOs), as coordinators of regional transportation decision-making, can promote regional business continuity after an emergency. The focus of the study is on the role of Transportation Demand Management strategies (TDMs) in supporting employee mobility and business continuity.

This paper summarizes the results of a 2008 study commissioned by the Sacramento Area Council of Governments, the MPO for three of California's urbanized areas. It represents the MPO's first step towards the development of an emergency management and business continuity plan for its six-county region. Based on 20 interviews with government agencies and private companies across the United States, as well as a review of government and industry publications, the paper highlights best practices—including public-private partnerships, resource sharing protocols, and technology applications—for maintaining employee mobility and business continuity following an emergency situation. The study also presents five case studies based on public and private sector experiences that highlight lessons learned and planning and coordination efforts aimed at supporting employee mobility after an emergency." [p. 1]

5.3.5 Regulatory Pressure on Technology for Business Continuity

Title: Regulatory Pressure on Technology for Business Continuity
Author(s): Brian J. Zawada
Organization: Unavailable
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 20-27
Retrieved from: Risk Management, Vol. 50, no. 7
Hyperlink: http://www.rmmag.com/Magazine/PrintTemplate.cfm?AID=2024
Date of Publication: July 2003

Abstract:
"Since the 1996 Critical Infrastructure Protection initiative, U.S. governmental and industry bodies have steadily increased the level of regulation for business continuity management. While these regulations go beyond the scope of information technology requirements, most call for heavy investment and development in technology and attention to its risks. Being prepared for technological failures, regardless of the cause, is not just good for business, it is the law. Attention to this matter has been spurred by a number of goals: to protect customers without the means to influence larger organizations' continuity processes; to safeguard the nation's critical infrastructure and ensure the continuity of critical services; to force organizations to establish mature, defined continuity programs; and to capture best practices and lessons learned from successful recoveries. Regulatory bodies are tasked with developing a set of guidelines that apply to all organizations and balance the benefits with the struggle to be compliant. As a result, regulatory requirements differ greatly in scope and depth. Some are industry independent, while others are industry specific. Some are new, while others are expansions of older guidelines. By understanding the regulations and incorporating related guidelines, risk managers and IT departments can assure that their companies are in compliance and prepared for technological and business failure." [p. 20]

6 Miscellaneous

Overview

The references presented in this chapter are discussion papers which examine critical infrastructure from political, social, legal and security perspectives and did not fall into the previous categorizations. The references are ordered chronologically, from most to least recent.

6.1 Resilience, Critical Infrastructure, and Molecular Security: The Excess of "Life" in Biopolitics

Title: Resilience, Critical Infrastructure, and Molecular Security: The Excess of "Life" in Biopolitics
Author(s): Tom Lundborg (Swedish Institute of International Affairs) and Nick Vaughan-Williams (University of Warwick)
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 367-383
Retrieved from: International Political Sociology, Vol. 5, Issue 4
Hyperlink:
http://www2.warwick.ac.uk/fac/soc/pais/people/vaughan-williams/publications/ips_dec_2011.pdf
Date of Publication: December 2011

Abstract:
"This article investigates the political significance of the orientation of Western security relations around critical infrastructure (CI) and resilience planning. While the analysis is located in the International Political Sociology literature, it departs from recent biopolitical accounts of CIs and resilience. These accounts tend to present such apparatuses as closed, totalizing, and inevitably ‘‘successful’’ modes of governance. Rather, we argue that resilient CIs are open, vulnerable, and often absurd systems that continually falter, backfire, and often undermine themselves according to their own logic. By developing what we call a ‘molecular security’’ approach, we draw attention to the way in which life constantly evades capture. In this sense, we suggest, there is always an excess of ‘‘life’’ in biopolitics." [p. 367]

6.2 National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience

Title: National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience
Author(s): Gail Ridley
Organization: International Centre for Corporate Social Responsibility, Nottingham University Business School
Publisher: University of Nottingham
Publishing Location: Nottingham, UK
Edition: N/A
Pages: 26
Retrieved from: No. 55-2010 International Centre for Corporate Social Responsibility Research Paper Series
Hyperlink: N/A
Date of Publication: 2010

Abstract:
"This paper argues for an extension to the scope of corporate social responsibility (CSR) research to include a contemporary issue of importance to national and global security, critical infrastructure resilience. Rather than extending the multiple perspectives on CSR, this study aimed to identify a method of recognising CSR-related issues, before applying it to two dissimilar case studies on critical infrastructure resilience. One case study was of an international telecommunications company based in the US while the other was of the railway network in Britain during a period of privatisation. The method used was derived from Okoye's (2009) common reference core for CSR. Both case studies satisfied all the criteria sought which points to critical infrastructure resilience as being an emerging CSR issue. Because ongoing change characterises CSR, the method may have application for identifying future new CSR strands. As the findings suggest that some aspects of national and global security are CSR-related phenomena, the study demonstrates how CSR research may be significant at a societal, national and global level. Implications of the study include a broadening of the value and reach of contributions from CSR researchers and practitioners." [p. 1]

Keywords: corporate social responsibility; national security; critical infrastructure resilience; case study; Microsoft Corporation; British railway industry; essentially contested concepts

6.3 The Legal Imperative to Protect Critical Energy Infrastructure

Title: The Legal Imperative to Protect Critical Energy Infrastructure
Author(s): Jacques J.M. Shore
Organization: Canadian Centre of Intelligence and Security Studies (CCISS) at Carleton University
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 16
Retrieved from: Critical Energy Infrastructure Protection, Policy Research Series, No. 2-2007-2008, from the Carleton University website
Hyperlink: http://www3.carleton.ca/cciss/ceipprs_publications/shore_02_2008.pdf
Date of Publication: March 2008

Description:

- This paper argues, "beyond the motivation to reduce threats to national and corporate security that both public and private sectors must share, another motivation in "securing the economy" is to guard against legal liability. In order to avoid or reduce potential legal liability, there is a legal imperative on the part of both government and private enterprise to protect CEI [Critical Energy Infrastructure]." [p. 3]

Additional Information:
This paper includes the following sections:

- The Responsibility of Government to Protect CEI
- Reducing Government Liability: The Legal Imperative to Protect CEI
- Reducing Corporate Liability: The Legal Imperative to Protect CEI

6.4 The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem

Title: The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem
Author(s): Stephen J. Collier and Andrew Lakoff
Organization: N/A
Publisher: Routledge
Publishing Location: New York
Edition: Unavailable
Pages: 34
Retrieved from: Chapter in *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitizatio*n. (Eds. Myriam Dunn and Kristian Søby Kristensen)
Hyperlink: http://anthropos-lab.net/wp/publications/2008/01/collier-and-lakoff.pdf
Date of Publication: 2007

Description:

- "In this chapter we ask: Where did this distinctive way of understanding and intervening in security threats come from? How did "critical infrastructure" come to be regarded as a national security problem? We argue that critical infrastructure protection is best understood as one response to a relatively new problematization of security…
- As we will show, at pivotal moments in the twentieth century, technological and political developments rendered prior security frameworks inadequate, and forced experts to invent new ways of identifying and intervening in security threats. Specifically, what emerged was a way of understanding security threats as problems of system-vulnerability. The task of protecting national security came to include attention to the ongoing functioning of a number of vulnerable systems that were seen as vital to collective life." [p. 4]
- "Our goal in tracing this history is to make this increasingly central approach to security problems available for critical scrutiny by analyzing its elements, and pointing to the contingent historical events and processes that shaped its formation." [p. 4]

7 Summary

This document presents the results of an extensive literature search for CI, performed as a part of a collaborative project between EMBC and DRDC. It is a collection of approximately 200 references, which includes government publications, academic research, and the work of non-governmental or private sector organizations. The organization and description of these references are intended to aid DRDC, EMBC and other partners in identifying and retrieving references that are most relevant to their work and interests.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, for example Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)
Centre for Security Science Defence R&D Canada 222 Nepean St. 11th Floor Ottawa, ON Canada K1A 0K2	UNCLASSIFIED (NON-CONTROLLED GOODS) DMC A Review: ECL June 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Critical Infrastructure References: Documented Literature Search

4. AUTHORS(last name, followed by initials – ranks, titles, etc. not to be used)

Pak, K., Genik, L

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
October 2012	214	7

7. DESCRIPTIVE NOTES (The category of the document, for example technical report, technical note or memorandum. If appropriate, enter the type of report, for example interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Note

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science

Defence R&D Canada

222 Nepean St. 11th Floor

Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
File 3700-1	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s).(Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS TN 2012-013	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unclassified/Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This document presents the results of a literature search on critical infrastructure (CI), an initiative undertaken by Defence Research and Development Canada (DRDC) as a part of its collaborative project with Emergency Management British Columbia (EMBC). The literature search document comprises a collection of approximately 200 references, including bibliographic information, abstracts, and content descriptions. In addition, the references are organized into the following categories: national approaches to CI; processes for managing CI; incident case studies and lessons learned; business continuity; and miscellaneous references. The references include government publications, academic papers, and the work of non-governmental and private sector organizations. These references were categorized, ordered, and described to allow readers to identify and retrieve references that are most valuable to their work and interests, and is thus intended to serve as a resource for DRDC, EMBC and other partners.

Le présent document expose les résultats d'une recherche documentaire sur les infrastructures essentielles (IE), une initiative de Recherche et développement pour la défense Canada (RDDC) dans le cadre de son projet de collaboration avec Emergency Management British Columbia (EMBC). La recherche documentaire comporte une collection d'environ 200 références, y compris des renseignements bibliographiques, des résumés et des descriptions de contenu. En outre, les références sont classées dans les catégories suivantes : approches nationales aux IE; processus de gestion des IE; études de cas d'incident et leçons apprises; continuité des activités; références diverses. Les références comprennent des publications gouvernementales, des documents universitaires et des travaux d'organismes non gouvernementaux et du secteur privé. Ces références ont été classées par catégories et ordonnées et ont fait l'objet de descriptions afin de permettre aux lecteurs de repérer et de récupérer les références les plus utiles pour ce qui est de leur travail et de leurs intérêts. Par conséquent, elles ont pour but de servir de ressources pour RDDC, EMBC et d'autres partenaires.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, for example Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Critical Infrastructure; Literature Search